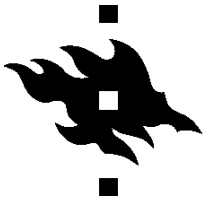

HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

Privacy Shield Redress Mechanisms

Assessment in the Light of the *Schrems* Case

University of Helsinki
Faculty of Law

Master's Thesis in European Law

April 2017

Author: Leena Salolatva

Supervisors: Emilia Korkea-Aho and Suvi Sankari

Tiedekunta/Osasto Fakultet/Sektion – Faculty Faculty of Law	Laitos/Institution– Department University of Helsinki	
Tekijä/Författare – Author Leena Salolatva		
Työn nimi / Arbetets titel – Title Privacy Shield Redress Mechanisms, Assessment in the Light of the *Schrems* Case		
Oppiaine /Läroämne – Subject European Law		
Työn laji/Arbetets art – Level Master's thesis	Aika/Datum – Month and year 04/2017	Sivumäärä/ Sidoantal – Number of pages 78

Tiivistelmä/Referat – Abstract

This research studies Adequacy Decisions, the Safe Harbour and the Privacy Shield, under which transfers of personal data from the European Union to the United States are facilitated. The focus is on 'redress mechanisms', thus the mechanisms under which EU citizens can seek redress or compensation against violations of data protection rules. The research assesses the redress mechanisms of the Privacy Shield in the Light of the Court of Justice of the European Union case *Schrems*. Firstly the Safe Harbour Decision and its redress mechanisms are introduced. Then the *Schrems* case where the Safe Harbour was invalidated is analysed. Focus is on what the Court says about redress mechanisms, and the criteria that it establishes for the assessment of Adequacy Decisions. This criteria is then applied to the Privacy Shield redress mechanisms.

According to the criteria, an Adequacy Decision must fulfil the requirements set out in Article 47 of the Charter of Fundamental Rights, thus right to an effective remedy and to a fair trial. The different redress mechanisms of the Privacy Shield are assessed in light of this Article by using case law of the Court of Justice of the European Union, as well as European Court of Human Rights. The study finds that all the redress mechanisms are not in line with Article 47. More specifically there are deficiencies in terms of the remedies available under different redress options, also all the procedures cannot be considered 'fair' as required by Article 47. More specifically, there is not always an opportunity for *inter partes* proceedings or a reasoned decision. Also the independence and impartiality of some of the dispute resolution bodies is questionable. Moreover, the complexity of the Privacy Shield redress mechanisms may in some situations mean that the time of the proceedings may exceed what would be considered reasonable from the perspective of European law.

The redress of mechanisms of the Privacy Shield rely heavily on Alternative Dispute Resolution (ADR). The compatibility with Article 47 of the Charter and ADR is not discussed as such, although the requirement of mandatory ADR before judicial dispute resolution is considered. Instead, the study asks whether the ADR mechanisms of the Privacy Shield could be compatible with Article 47.

This study is done from a European perspective, thus focusing on EU fundamental rights. Study of laws of the United States are left outside the scope of the research, although some references are made. Similarly the study of redress mechanisms is limited to those introduced in the Privacy Shield and routes to seek redress in US courts are excluded. The aim of this study is thus to assess whether the Privacy Shield would pass the criteria established by the Court of Justice of the European Union in its *Schrems* case. The study takes a fundamental right perspective, although it does recognize that European data protection law does have other objectives other than the protection of personal data, such as economic objectives.

Avainsanat – Nyckelord – Keywords
Privacy Shield, Safe Harbour, data protection, redress, European Union, United States, Schrems, data transfer

Säilytyspaikka – Förvaringställe – Where deposited
Helsinki University Library

Muita tietoja – Övriga uppgifter – Additional information

Table of Contents

Sources

Journal Articles

Azoulai, Loïc and van der Sluis, Marijn, Institutionalizing personal data protection in times of global institutional distrust: Schrems, *Common Market Law Review*, Vol. 53, Issue 5, (2016), pp. 1343–1372

Blanke, Jordan M., "Safe Habor" and the European Union's Directive on Data Protection, 11 *Albany Law Journal of Science and Technology*, 57, (2000-2001)

Brkan, Maja, The Unstoppable Expansion of the EU Fundamental Right to Data Protection, Little Shop of Horrors? *Maastricht Journal of European and Comparative Law* 2016, Vol. 23(5), pp. 812-841

Deighton, Alison, The EU-US Privacy Shield - is it strong enough?, *Privacy & Data Protection*, 2016, 16(4), 8-10

DiLascio, Tracey, How Safe is the Safe Harbor? U.S. and E.U. Data Privacy Law and the Enforcement of the FTCs Safe Harbor Program, *Boston University International Law Journal*, vol. 22, 399, 2004

Frantziou, Eleni, Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12, Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos, *Human Rights Law Review*, 2014, 14, 761–777

Gonzáles Fuster, Gloria, Un-mapping Personal Data Transfers, 2 *European Data Protection Law Review*, 160, (2016)

Greenleaf, Graham, The influence of European data privacy standards outside Europe: implications for globalization of Convention 108, *International Data Privacy Law*, 2012, Vol. 2, No. 2, pp. 68–92

Hoofnagle, Chris Jay, US Regulatory Values and Privacy Consequences, Implications for the European Citizen, 2 *European Data Protection Law Review* 169 (2016)

Jeretina, Urša and Uzelac, Alan, Alternative Dispute Resolution for Consumer Cases: Are Divergences an Obstacle to Effective Access to Justice? *Mednarodna Revija za Javno Upravo/International Public Administration Review December* 2014, Vol.12(4), pp.39-74

Khan, Sana, Invalidity of EU–US Safe Habor: practical implications: Part 1, *Compliance & Risk*, 2016, 5(2), 2–7

Khan, Sana, Invalidity of EU–US Safe Habor: practical implications: Part 2, *Compliance & Risk*, 2016, 5(3), 10-12

Kobrin, Stephen J. Safe harbours are hard to find: The trans-Atlantic data privacy dispute, territorial jurisdiction and global governance, *Review of International Studies*, (2014), 30, 111–131, p. 116–117.

Kuner, Christopher, Reality and Illusion in EU Data Transfer Regulation Post Schrems, Legal Studies Research Paper Series, *University of Cambridge Faculty of Law*, Paper No. 14/2016, March 2016, p. 9.

Markel, Mike, Safe Harbor and Privacy Protection: A Looming Issue for IT-professionals, *IEEE Transactions on Professional Communication*, vol. 49, no. 1, March 2006, p. 1.

Meltzer, Joshua Paul, The Internet, Cross-border Data Flows and International Trade, *Asia &Pacific Policy Studies*, vol. 2, no. 1, 2014, pp. 90–102.

Mouzakiti, Foivi, Transborder Data Flows 2.0.: Mending the Holes of the Data Protection Directive, *European Data Protection Law Review*, vol. 1, 39, 2015, p. 51.

NiLoidean, Nora, The End of Safe Harbor: Implications for EU Digital Privacy and Data Protection Law, 19, No. 8, *Journal of Internet Law* 1, February 2016,

Reidenberg, Joel L., E-Commerce and Trans-Atlantic Privacy, 38 *Houston Law Review* 717 2001-2002, p. 718.

Rotenberg, Marc and Jacobs, David, Updating The Law on Information Privacy: The New Framework of the European Union, *Harvard Journal of Law & Public Policy*, vol. 36, 605, 2013, p. 638.

Schrems, Max, The Privacy Shield is a Soft Update of the Safe Harbor, 2 *European Data Protection Law Review*, 148, (2016)

Ustaran, Eduardo, Privacy Shield Explained: Part 2, *Privacy & Data Protection*, (2016), 16(6), 3–4

Ustaran, Eduardo, Privacy Shield Explained: Part 3, *Privacy & Data Protection*, (2016), 16(7), 3–4

Varney, Mike, effective Redress of Grievance in Data Protection: An Illusion?, *Maastricht journal of European and comparative law*, Vol.23(3), pp. 550–567.

Varotto, Stefano, The Schrems decision, the EU-US Privacy Shield and the necessity to rethink how to approach cross border personal data transfers at global level, *Communications Law*, 2016, 21(3), 78-87

Online Articles

Greenwald, Glenn, NSA collecting phone records of millions of Verizon customers daily, The Guardian, 6 June 2013, available at: <https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order> accessed on 26 Jan 2017

Kuner, Christopher, (2011), "Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future", OECD Digital Economy Papers, No. 187, OECD Publishing, Paris, <http://dx.doi.org/10.1787/5kg0s2fk315f-en> accessed on 31 march 2017.

Kuner, Christoprer, The Sinking of the Safe Harbor, 8.10.2015, VerfBlog available at <http://verfassungsblog.de/the-sinking-of-the-safe-harbor-2/> accessed on 6 March 2017

Schwent, Jason and Ventrone, Melissa, Has Trump dumped privacy protections for EU citizens?, 14.2.2017, available at: <http://www.jdsupra.com/legalnews/has-trump-dumped-privacy-protections-57553/> accessed on 22.2.2017

Warren, Samuel, and Brandeis, Louis, The Right to Privacy, Harvard Law Review, Vol. IV, December 15, 1890, No. 5, available at <http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html> accessed on 26 Jan 2017.

Books

Born, Gary B., International Arbitration: Cases and Materials, 2nd edition, Kluwer Law International, (2014)

Bräutigam, Tobias, The Land of Confusion: International Data Transfers Between Schrems and the GDPR, in Data Protection, Privacy and the European Regulation in the Digital Age, Bräutigam, Tobias and Miettinen, Samuli, (eds.), Unigrafia, Helsinki 2016, pp. 143–177

Davies, Simon, Privacy Opportunities and Challenges with Europe's New Data Protection Regime, in Totenberg, Marc et al, Privacy in the Modern Age, The Search for Solutions, The New Press, New York, United States 2015, pp. 55–60

Glanert, Simone, Method? in Methods of Comparative Law, Monateri, Pier Giuseppe, Edward Elgar Publishing Limited, Cheltenham, UK, Northampton, Massachusetts, USA, 2012, pp. 61–81

González Fuster, Gloria, The emergence of personal Data Protection as a Fundamental Right of the EU, Law, Governance and Technology Series vol. 16, Springer International Publishing Switzerland 2014

Hirvonen, Ari, Mitkä metodit? Opas oikeustieteen metodologiaan, Yleisen oikeustieteen julkaisuja 17, Helsinki 2011

Hopt, Klaus J. and Steffek, Felix, Mediation: Comparison of Laws, Regulatory Models, Fundamental Issues, in Hopt, Klaus J. and Steffek, Felix (Eds.), Mediation: Principles and Regulation in Comparative Perspective, Oxford University Press, Oxford, United Kingdom, 2013, pp. 5–121.

Irion, Kristina, Accountability Unchained: Bulk Data Retention, Preemptive Surveillance, and Transatlantic Data Protection, in Totenberg, Marc et al, Privacy in the Modern Age, The Search for Solutions, The New Press, New York, United States 2015, pp. 78–92.

Koskenniemi, Martti, The Effect of Rights on Political Culture, in Alston, Philip, Bustelo, Mara, Heenan, James (Eds.) The EU and Human Rights, Oxford University Press, New York, United States, 1999, pp. 99–116.

Kuner, Christopher, Developing an Adequate Legal Framework for International Data Transfers, in Reinventing Data Protection?, Gutwirth, Serge et al (Eds.), Springer 2014, p. 263–273.

Kuner, Christian, European Data Protection Law, Corporate Compliance and Regulation, Oxford University Press, New York, 2nd. Ed. 2007, p. 81–83.

Kuner, Christopher, Transborder Data Flows and Data Privacy Law, Oxford University Press, Oxford, United Kingdom 2013, 1st Ed.

Case law of the Court of Justice of the EU

Case C-106/77, Amministrazione delle Finanze dello Stato v Simmenthal SpA, EU:C:1978:49

Case C-213/89, The Queen v Secretary of State for Transport, ex parte: Factortame Ltd and others, EU:C:1990:257,

Case C-24/92, Pierre Corbiau v Administration des contributions, EU:C:1993:118

Case C-312/93, Peterbroeck, Van Campenhout & Cie SCS v Belgian State, EU:C:1995:437

Case C-54/96, Dorsch Consult Ingenieurgesellschaft mbH v. Bundesbaugesellschaft Berlin mbH, EU:C:1997:413

Case C-101/01, Criminal proceedings against Bodil Lindqvist, EU:C:2003:596

Case C-506/04, Graham J. Wilson v Ordre des avocats du barreau de Luxembourg, EU:C:2006:587

Joined cases C-341/06 P and C-342/06 P, Chronopost SA and La Poste v Union française de l'express (UFEX) and Others, EU:C:2008:375

Case C-73/07, Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy, EU:C:2008:727

Case C‑518/07, European Commission v Federal Republic of Germany, EU:C:2010:125

Case C-58/08, The Queen, on the application of Vodafone Ltd and Others v Secretary of State for Business, Enterprise and Regulatory Reform, EU:C:2010:321

Joined Cases C‑317/08, C‑318/08, C‑319/08 and C‑320/08, Rosalba Alassini v Telecom Italia SpA (C-317/08), Filomena Califano v Wind SpA (C-318/08), Lucia Anna Giorgia Iacono v Telecom Italia SpA (C-319/08) and Multiservice Srl v Telecom Italia SpA (C-320/08), EU:C:2010:146

Joined Cases C-92/09 and C-93/09, Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v Land Hessen, EU:C:2010:662

Case C-543/09, Deutsche Telekom AG v Bundesrepublik Deutschland, EU:C:2011:279

Joined Cases C‑584/10 P, C‑593/10 P and C‑595/10 P, European Commission and Others v Yassin Abdullah Kadi, EU:C:2013:518

Case C‑619/10, Trade Agency Ltd v Seramico Investments Ltd, EU:C:2012:531

Case C‑199/11, Europese Gemeenschap v Otis NV and Others, EU:C:2012:684

Case C‑300/11, ZZ v Secretary of State for the Home Department, EU:C:2013:363

Case C-399/11, Stefano Melloni v Ministerio Fiscal, EU:C:2013:107

Case C‑583/11 P, Inuit Tapiriit Kanatami and Others v European Parliament and Council of the European Union, EU:C:2013:625

Case C‑58/12 P, Groupe Gascogne SA v European Commission, EU:C:2013:770

Case C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Judgement of the Court (Grand Chamber), EU:C:2014:317

Case C‑291/12, Michael Schwarz v Stadt Bochum, EU:C:2013:670

Case C-293/12, Digital Rights Ireland and Seitlinger and Others, EU:C:2014:238

Case C‑567/13, Nóra Baczó and János István Vizsnyiczai v Raiffeisen Bank Zrt, EU:C:2015:88

Case C‑362/14, Maximillian Schrems v Data Protection Commissioner, joined party: Digital Rights Ireland Ltd, EU:C:2015:650 (Case C‑362/14, *Schrems* case)

Case T-670/16, Digital Rights Ireland v Commission, OJ C 410 from 07.11.2016, p.26

Case T-738/16, La Quadrature du Net and Others v Commission, OJ C 6 from 09.01.2017, p.39.

Advocate General Opinions

Opinion of Advocate General Bot, EU:C:2015:627, delivered on 23 September 2015 (1), Case C‑362/14, Maximillian Schrems v Data Protection Commissioner

Case law of the European Court of Human Rights

ECtHR, Campbell and Fell v. the United Kingdom, No. 7819/77; 7878/77, 28 June 1984

ECtHR, König v. Germany, No. 6232/73, 28 June 1978.

ECtHR, Klass and others v Germany, No. 5029/71, 6 September 1978

ECtHR, Poiss v. Austria, No, 9816/82, 23 April 1987

ECtHR, Hadjianastassiou v. Greece, No. 12945/87, 16 December 1992

ECtHR, Ruiz-Mateos v. Spain, No. 12952/87, 23 June 1993

ECtHR, Frydlender v. France, No. 30979/96, 27 June 2000

ECtHR, Suominen v. Finland, No. 37801/97, 24 July 2003

ECtHR, Kennedy v. the United Kingdom, No. 26839/05, 18 August 2010

ECtHR, Vučković and Others v. Serbia, No. 17153/11 and 29 other cases, 25 March 2014

Other case law

Maximillian Schrems v Data Protection Commissioner, [2013 No. 765JR], [2014], IEHC 310

EU Legislation

European Convention on Human Rights, Rome, 4.XI.1950

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Strasbourg, 28.I.1981 (Convention 108)

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal L 281 , 23/11/1995 (Data Protection Directive)

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

The Charter of Fundamental Rights of the European Union (2012/C 326/02), OJ C 326, 26.10.2012, p. 391–407 Official Journal of the European Communities, C 364/20 (the Charter)

Treaty on European Union, OJ C 326, 26.10.2012, p. 13–390

Treaty on the Functioning of the European Union, OJ C 326, 26.10.2012, p. 13–390

US Legislation

Judicial Redress Act 2015, Public Law, 114–126—FEB. 24, 2016, available at: <https://www.congress.gov/114/plaws/publ126/PLAW-114publ126.pdf> accessed on 22 April 2017

Federal Trade Commission Act, Incorporating U.S. SAFE WEB Act amendments of 2006, Sec. 5. available at: <https://www.ftc.gov/enforcement/statutes/federal-trade-commission-act> accessed on 2 March 2017

Foreign Intelligence Surveillance Act 2008, 50 U.S. Code Chapter 36. available at: <https://www.govtrack.us/congress/bills/110/hr6304/text> accessed on 22 April 2017 (FISA)

Freedom of Information Act 2016, available at: <https://www.justice.gov/oip/freedom-information-act-5-usc-552> accessed on 22 April 2017 (FOIA)

International Treaties etc.

‘The Safe Harbour Decision’ 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) (Text with EEA relevance.) Official Journal L 215 , 25/08/2000 P. 0007 – 0047.

‘The Privacy Shield Decision’ Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (notified under document C(2016) 4176) (Text with EEA relevance), C/2016/4176.

OECD Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (23 September 1980) (updated in 2013), <https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm> accessed on 25 Jan 2017

Official Documents etc.

Article 29 Data Protection Working Party

Article 29 Working Party Rules of Procedure, Brussels, 15 February 2010, available at: < http://ec.europa.eu/justice/data-protection/article-29/files/rules-art-29_en.pdf> accessed on 22 April 2017.

Article 29 Data Protection Working Party tasks, available at: <http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083> accessed on 23 January 2017.

‘WP29 Opinion 4/2000’ Article 29 Data Protection Working Party Opinion 4/2000 on the level of protection provided by the “Safe Harbor Principles” Adopted on 16th May 2000, CA07/434/00/EN WP 32.

‘WP29 Opinion 01/2016’ Article 29 Data Protection Working Party, Opinion 01/2016 on the EU–U.S. Privacy Shield draft adequacy decision, Adopted on 13 April 2016, 16/EN, WP 238

‘WP29, *Schrems* Statement’ Statement of the Article 29 Working Party, Statement on the implementation of the judgement of the Court of Justice of the European Union of 6 October 2015 in the Maximilian Schrems v Data Protection Commissioner case (C-362-14), Brussels, 16 October 2015, <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm> accessed on 8 Feb 2017.

‘WP29 Working Document’ Article 29 Working Party Working Document, Working Party on the Protection of Individuals with regard to the Processing of Personal Data, Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive, Adopted by the Working Party on 24 July 1998.

European Commission

European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century, Brussels, 25.1.2012 COM(2012) 9 final

European Commission, Guide to the EU–U.S. Privacy Shield, Directorate-General for Justice and Consumers, European Union 2016, available at <http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm> accessed on 15 Feb 2017.

European Commission, MEMO/15/6385, Fact Sheet, Questions and Answers - Data protection reform, Brussels, 21 December 2015, available at: <http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm> accessed on 24 Feb 2017

European Commission, MEMO/16/2462, Fact Sheet, EU–U.S: Privacy Shield: Frequently asked Questions, Brussels, 12 July 2016, available at: <http://europa.eu/rapid/press-release_MEMO-16-2462_en.htm> accessed on 8 Feb 2017.

European Commission, Press release, IP/16/216, EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield, Strasbourg, 2 February 2016, available at: <http://europa.eu/rapid/press-release_IP-16-216_en.htm> accessed on 8 Feb 2017.

European Commission, Press release, IP/16/2461, European Commission launches EU-U.S. Privacy Shield: stronger protection for transatlantic data flows, Brussels, 12 July 2016, available at: <http://europa.eu/rapid/press-release_IP-16-2461_en.htm> accessed on 8 Feb 2017.

Other

Cisco, The Zettabyte Era: trends and Analysis, White Paper, June 2016, available at: <http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html> accessed on 6 April 2017.

'ECIPE report' The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce, European Centre for International Political Economy, Brussels, Belgium, March 2013, available at: <https://www.uschamber.com/sites/default/files/documents/files/020508_EconomicImportance_Final_Revised_lr.pdf> accessed on 22 April 2017.

Executive Order: Enhancing Public Safety in the Interior of the United States, 25 Jan 2017, White House, Office of the Press Secretary, available at: <https://www.whitehouse.gov/the-press-office/2017/01/25/presidential-executive-order-enhancing-public-safety-interior-united> accessed on 22 Feb 2017

'From Safe Harbour to Privacy Shield', Monteleone, Shara and Puccio, Laura, From Safe Harbour to Privacy Shield, Advances and shortcomings of the new EU-US data transfer rules, In-Depth Analysis, EPRS, European Parliamentary Research Service, European Union, 2017.

Handbook on European law relating to access to justice, European Union Agency for Fundamental Rights and Council of Europe, Luxembourg: Publications Office of the European Union, (2016)

Letter to Vice President Reding, Article 29 Data Protection Working Party, Brussels, 10 April 2014, Ref. Ares(2014)1139376 - 10/04/2014, available at <http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140410_wp29_to_ec_on_sh_recommendations.pdf> accessed on 6 March 2017

Privacy Bridges, EU and US Privacy Experts in Search of Transatlantic Privacy Solutions, 37th International Privacy Conference Amsterdam, Amsterdam/Cambridge (2015), available at <https://privacybridges.mit.edu/> accessed on 13 March 2017

Websites

Commission decisions on the adequacy of the protection of personal data in third countries, Website of the European Commission, available at: <http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm> accessed on 19 January 2017.

Data Protection Authorities list, available at: <http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm> accessed on 10 April 2017.

Department of Commerce website, About Commerce, available at: <https://www.commerce.gov/page/about-commerce> accessed on 28 March 2017.

EU Charter of Fundamental Rights, website of the European Commission, <http://ec.europa.eu/justice/fundamental-rights/charter/index_en.htm> accessed on 5.1.2017.

FTC complaints on FTC website, available at: <https://www.ftccomplaintassistant.gov/#&panel1-1> accessed on 15 Feb 2017.

GDPR website, available at: <http://www.eugdpr.org/eugdpr.org.html> accessed on 16 March 2017.

Legal Information Institute website, available at: <https://www.law.cornell.edu/wex/alternative_dispute_resolution> accessed on 10 April 2017

NSA website, available at: <https://www.nsa.gov/> accessed on 17 March 2017.

Oxford English Dictionary online, available at: <http://www.oed.com/view/Entry/160455?rskey=p2mx7w&result=1#eid> accessed on 16 March 2017.

Reform of EU data protection rules, available at: <http://ec.europa.eu/justice/data-protection/reform/index_en.htm> accessed on 22 March 2017.

TURSTe website, TRUSTe Privacy Dispute Resolution FAQs, available at <https://www.truste.com/consumer-resources/dispute-resolution/dispute-resolution-faqs/#whofile> accessed on 28 Feb 2017.

The Online Dispute Resolution form in TRUSTe Feedback and Resolution System, available at: <https://feedback-form.truste.com/watchdog/request> accessed on 28 Feb 2017.

Abbreviations

ADR – Alternative Dispute Resolution

CJEU – Court of Justice of the European Union

DoC – Department of Commerce

DPA – Data Protection Authority

DPD – Data Protection Directive

ECHR – European Convention on Human Rights

ECtHR – European Court of Human Rights

EU – European Union

FISA – Foreign Intelligence Surveillance Act

FOIA – Freedom of Information Act

FTC – Federal Trade Commission

GDPR – General Data Protection Regulation

NSA – National Security Authority

TEU – Treaty on the European Union

TFEU – Treaty on the Functioning of the European Union

US – United States

WP29 – Article 29 Working Party

1. Introduction

1.1. Significance of EU Data Protection

Data has become very important in today's digitalized world. The European Commission calls it 'the currency of today's digital economy'.[1] Many 'free' online services, such as Facebook or Google search, are actually funded by collecting personal data of the people who use these services. Personal data has immense economic value and potential. The free flow brings many benefits to the society at large allowing the realization of many values, such as freedom of expression, economic growth or disaster relief. Individuals also benefit from the wide variety of services offered to them. In the modern world individual states have become more interdependent and the flow of data across borders allows development in many areas, governments need to co-operate with each other.[2] Overall data flows can bring prosperity and thus be beneficial to all.

For the European Union, the United States is arguably one of the most important trading partners. Data flows between across the Atlantic can multiply trade and bring remarkable economic gains. That marketplace consist of for half of world GDP with addition to 2,4 trillion euros worth of bilateral investments.[3] The exact amount of data crossing the Atlantic may be impossible to calculate, but statistics certainly support the view that internet data traffic is on the rise.[4] The substantial growth of cross-border data flows have also been recognised at the EU. The data protection law reform that is ongoing in the Union specifically mentions the importance technological developments and their influence to social and economic integration and the rapid growth of data flows.[5]

Despite all these economic advantages, there are also threats to the privacy of individual EU citizens, as well as national governments or businesses.[6] For individuals, who are the main

[1] European Commission, MEMO/15/6385, (2015).
[2] Kuner, (2013), pp. 102–103.
[3] ECIPE Report, (2013), p. 6.
[4] Cisco, White Paper, (2016).
[5] Preamble, paras. 5–6, Regulation (EU) 2016/679, (General Data Protection Regulation),
[6] Kuner, (2013), pp. 103–104.

interest of this thesis, processing of their personal data can also lead to tragic results, such as public embarrassment, risk of financial loss or decisions that affect the life of the individual, credit granting or recruitment.[7] Most commonly, data is collected when individuals use online services. Companies and organisations then use it to their advantage, e.g. for targeted marketing, or the data can be even sold on to different companies. Oftentimes the individual does not even know what data different companies might have, and for what purpose it is being used. Technological advancements have been seen as threats to privacy, not just the recent rise of internet and the mass collection of personal data online, but for instance the development of photography in the late 19th century caused concerns for the privacy of an individual human being. Warren and Brandeis argued already in 1890 in their famous article, that privacy is right that every individual inherently has. Also they though that interference with this privacy should be remedied.[8] This is why data protection legislation is needed.

EU data protection legislation has two objectives. On the other hand it seeks to ensure the free flow of personal data and, on the other it seeks to protect privacy, thus more specifically there is protection of personal data. The objectives are enshrined also in secondary EU data protection legislation.[9] Although this research is not directly concerned of the objectives of the data protection legislation, they are, nevertheless issues that must be borne in mind, while discussing data protection.

European data protection legislation is the most developed in the world. In fact, data protection is a fundamental right according to Article 8 of the Charter of Fundamental Rights (hereinafter referred to as the Charter), which states:

> 1. Everyone has the right to the protection of personal data concerning him or her.
>
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
>
> 3. Compliance with these rules shall be subject to control by an independent authority[10]

[7] Kuner, (2013), pp. 104–105.
[8] Warren and Brandeis, (1890).
[9] See e.g. Art. 1 Directive 95/46/EC, Data Protection Directive, and Art. 1, General Data Protection Regulation.
[10] Art. 8, Charter of Fundamental Rights.

European data protection is based on the idea of autonomy or self-determination.[11] This means, in the context of the EU, that the data can be collected for specified legitimate purpose and processed fairly.[12] The data protection rules would be empty if they could not be enforced. Individuals must have the opportunity to enforce the right and also seek compensation when the rules are violated.

Therefore ensuring effective redress is essential in giving effect to the right of data protection. By 'redress mechanisms' I mean the mechanisms, or the ability or opportunity of EU citizens to seek some form of compensation or remedy in case there is a violation or breach of the data protection rules. The Commission also recognizes that ensuring effective redress in data protection issues is essential in guaranteeing the right.[13] To effectively ensure the ability to seek redress it is essential to guarantee means to seek it, which could be judicial or non-judicial. The traditional option is in front of a court, that the can afford a monetary compensation, but different out-of-court options, such as arbitration or mediation can sometimes be equally good, if not even better. Also, effective remedies do not necessarily need to be monetary. The non-judicial redress options are called Alternative Dispute Resolution (ADR).

An important provision is Article 47 of the Charter that protects the access to justice and also effective remedy. It states:

> Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article.
>
> Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law. Everyone shall have the possibility of being advised, defended and represented.
>
> Legal aid shall be made available to those who lack sufficient resources in so far as such aid is necessary to ensure effective access to justice.[14]

[11] It is considered that individuals must have effective control over their personal data online. See e.g. Communication from the Commission, 25.1.2012, p. 2.
[12] See e.g. Art. 6(1), Data Protection Directive, and Art. 5(1), General Data Protection Regulation.
[13] Communication from the Commission, 25.1.2012, p. 6
[14] Art. 47, Charter of Fundamental Rights.

This provision is essential in guaranteeing the right of data protection (Article 8 of the Charter) in the last place. Whether Article 47 is compatible with non-judicial ADR mechanisms is a complicated issue, which is not the main focus of this study.

In the context of the EU, equally important to Article 47 of the Charter is Article 6 of the European Convention on Human Rights (hereinafter referred to as ECHR), which guarantees everyone the right to a fair trial. Article 6.1 of the ECHR states:

> In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. Judgment shall be pronounced publicly but the press and public may be excluded from all or part of the trial in the interests of morals, public order or national security in a democratic society, where the interests of juveniles or the protection of the private life of the parties so require, or to the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice.[15]

The Charter and the Convention have a very close relationship and corresponding rights have the same meaning. Also the case law of the European Court of Human Rights (hereinafter referred to as ECtHR) is equally important in the context of the EU as the Court of justice of the EU (hereinafter referred to as CJEU) case law in the interpretation of these provisions.[16] Access to fair trial and right to an effective remedy ensure the effectiveness of the fundamental right of protection of personal data. By 'effectiveness' I merely mean what it means in the context of Article 47 of the Charter, thus an effective remedy.

However, when data is transferred across the Atlantic to the United States, there is a problem. The question is whether the protection can extend also to situations where data is transferred to third countries. According to the European Commission it should extend.[17] The US approach to protection of personal data is different from the EU thinking of protecting personal data as a fundamental right. Certain data is seen as a commodity that the data subject can choose to reveal, and it can be traded for another good. Individual is responsible for his or her own data.[18]

[15] Art. 6.1, European Convention on Human Rights
[16] Handbook on European law relating to access to justice, (2016), pp. 11–13. See also Preamble, Charter of Fundamental Rights.
[17] Communication form the Commission, 25.1.2012, p. 10–11.
[18] Markel, (2006), p. 1. See also Kobrin, (2014), p. 116–117.

Industry self-regulation and technological mechanisms are a norm in the US, which differs vastly from the European approach to data protection.[19] Data protection laws in the US are piecemeal, sectoral and generally only apply to public institutions and not private ones.[20] The approach is thus rather 'market protecting' than 'individual protecting'.[21] A particularly big blow to the safety of personal data online came after the revelations of Edward Snowden in 2013. Snowden revealed that US authorities has a surveillance programme called Prism, which allowed US government's National Security Agency (NSA) to tap some leading internet firms, such as Facebook, Google and Microsoft, which have access to personal data of EU citizens.[22] The Snowden revelations created distrust towards US data collectors and processors. The US approach being so different ensuring EU level of data protection when data is transferred seems difficult.

EU has solved this problem by allowing transfers of personal data from the Union to third countries only when the third country in question has adequate level of data protection. From the perspective of the EU the US data protection laws are not adequate. Thus the EU and the EU have a bilateral agreement that established a regime under which transfers of personal data could take place. In this study, such an agreement is called an 'Adequacy Decision'. The first Adequacy Decision was called 'Safe Harbour' and it was recently replaced by a new regime called 'Privacy Shield'.

1.2. Scope of the Study

In this research I shall study the aforementioned Safe Harbour and the Privacy Shield. I am going to compare them and assess the changes that have been made. But I will not study all the aspects of these agreements, but rather I shall focus only on so called redress mechanisms. This is significant because, as already discussed above, the effectiveness of the data protection rules

[19] Reidenberg, (2001-2002), p. 726.
[20] Blanke, (2000-2001), p. 66.
[21] See e.g. Reidenberg, (2001-2002), p. 726 and 731.
[22] Greenwald, (2013). See also: Khan, Part 1, (2016), p. 4.

is largely dependent on their enforcement. And the rules would be meaningless for the individuals if they could not get any compensation for the loss suffered as a result of violation of the rules.

The new Privacy Shield, which recently replaced the Safe Harbour regime is meant to correct the flaws and deficiencies of the Safe Harbour. Amongst other things it is meant to provide better protection and easier redress.[23] I am going to assess whether it really does that. At the centre of my research is the CJEU case that invalidated the Safe Harbour, the *Schrems*.[24] In the case the Court established a criteria to assess Adequacy Decision such as the Privacy Shield or the Safe Harbour. Article 47 of the Charter which I mentioned above is an important element in the CJEU's decision. Max Schrems himself (the applicant in the *Schrems* case) has his reservations whether the Privacy Shield actually delivers everything that it says it does.[25]

Hence, the objective is to apply these criteria to the Privacy Shield to assess the effectiveness of the redress mechanisms. Firstly, I shall look at the Safe Harbour, more specifically the redress mechanisms and the *Schrems* case and see why the Safe Harbour failed. Then I shall compare the redress mechanisms of the Safe Harbour to the ones in the Privacy Shield and see if there is any improvement. As will be seen, the Privacy Shield (and the Safe Harbour) rely heavily on Alternative Dispute Resolution (ADR). The compatibility of this type of redress with Article 47 is not, as stated, the main focus. Therefore I shall not directly question whether ADR can be effective as opposed to a court. This thesis is not meant to enter the discussion about whether disputes are better solved by judicial or non-judicial means. Instead, I only assess the ADR options offered in light of the *Schrems* criteria, without comparing whether judicial means would be more effective. Hence I am open to the idea that ADR can be as effective.

With these considerations the research questions shall be the following:

1. What changes has the Privacy Shield introduced in terms of redress mechanisms in comparison to the Safe Harbour?

2. Would the Privacy Shield pass the test established by the CJEU in the *Schrems* case on part of the redress mechanisms?

[23] European Commission, Press release, IP/16/2461, 12 July 2016.
[24] Case C‑362/14, Maximillian Schrems v Data Protection Commissioner, joined party: Digital Rights Ireland Ltd. (Case C‑362/14, *Schrems* case)
[25] Schrems, (2016), p. 148.

The study is limited to assessing the Privacy Shield (and the Safe Harbour). While recognising that EU citizens ability to seek compensation for data protection violations may not be limited to the options listed in the Privacy Shield, for research economic reasons I shall limit my research. Redress mechanism outside the Privacy Shield are not assessed. For this reason I will not look very deep into US legislation, for instance, although I will make references to it throughout the thesis. My point of view in this study is European. Hence, I shall be discussing the issues from the perspective of EU law and perhaps most importantly fundamental rights. I am interested in the protection of personal data of EU citizens.

In addition to the fundamental rights perspective, the economic perspective is perhaps equally important when it comes to data protection. As mentioned EU data protection legislation has two objectives, the protection of data and free flow of data to realise its economic advantages. There is a tension between these two objectives, and neither of them can be fully attained. Too protectionist approach is going to stop the flow of data and lead to economic loss and the opposite approach of allowing the free flow without any limitations undermines individual privacy. This is an important factor to consider also remember that the CJEU case law could also has its effect on the economy, especially if it set the standard of protection too high. However, this study is mainly focused on the fundamental rights aspect. I shall only refer to the implications on economy towards the end of this thesis.

The study of redress mechanisms is also interesting because there are two applications pending at the CJEU. The Court has not given decisions, but when it does, it will likely to answer question about the effectiveness of redress mechanisms under the Privacy Shield. The two application have been put forward by Digital Rights Ireland and La Quadrature du Net.

Digital Rights Ireland, an Irish interest group, has filed an application for annulment at the CJEU of Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 of the so called Privacy Shield decision.[26] In its action the group has presented ten pleas of law, of which only the two that are relevant here shall be discussed. They argue *inter alia* certain provisions of a US law FISA Amendments ACT 2008[27] that allows authorities to access content of electronic communications is not concordant with Article 47 of the Charter of Fundamental Rights, the right to an effective remedy and a fair trial. Secondly they also argue that the Privacy Shield

[26] Case T-670/16, Digital Rights Ireland v Commission.
[27] Foreign Intelligence Surveillance Act 2008.

Decision denies Europeans the right to an effective remedy contrary to the Charter of Fundamental Rights and the General Principles, insofar as the decision allows access of public authorities to data or alternatively fails to provide adequate safeguards against such access and fails to provide an effective remedy.[28]

Also a French group, called La Quadrature du Net, which also promotes data protection rights, has also brought and action for annulment of the Privacy Shield. They are arguing that the Privacy Shield is contrary to Articles 7, 8 and 47 of the Charter. Their first argument is that the US regime is contrary to the essence of Article 7. Secondly, they argue that the Privacy Shield does not guarantee the protection of fundamental rights equivalent to EU standards. Thirdly, US regulatory regime does not provide an effective remedy, thus it is not equivalent. And finally the Privacy Shield is wrong because it does not assure protection which is equivalent (to EU protection).[29]

1.3. Data Protection Terminology

For the purposes of this research it is useful to discuss some terminological issues. My choice of terminology is European rather than American. 'Data protection' is better known as '(data) privacy' in the United States. The reasons for this difference lie in the historical development of data protection. In the US the beginnings of the concept were in privacy considerations, whereas the European data protection rules were inspired by the German term *Datenschutz* where it was translated into the English version of data protection.[30] Further discussions about the differences in terminology on the sides of the Atlantic is not required but here it is just useful to note that in this research I will be using the European term data protection.

Then data, or more specifically 'personal data' has to be defined. As the interest of this research is on the redress mechanism offered to individuals in case of data breaches in transatlantic data transfer situations, it is only 'personal data' that is at the centre of the study. Thus mere data or data that is not personal is not considered here. 'Personal data' refers to according to the Data

[28] Case T-670/16, Digital Rights Ireland v Commission.
[29] Case T-738/16, La Quadrature du Net and Others v Commission.
[30] Gonzáles Fuster, (2014), p. 56

Protection Directive ‘any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity’.[31] The GDPR definition of ‘personal data’ is similar but some factors have been added, namely ‘a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person’.[32] Hidden in the definition of data protection is also a term ‘data subject’, the natural person to whom the data in question refers to.

‘Data transfer’ happens when data is transferred from one country to another, transfer to a third country in the European context mean transfers to countries outside the EU. According to Organisation for Economic Co-operation and Development (OECD) Privacy Guidelines, transborder flows of data mean movement of data across national borders.[33] The first European piece of data protection legislation, Convention 108 Article 12(1) on the other hand defines it as a ‘transfer across national borders, by whatever medium, of personal data undergoing automatic processing or collected with a view to their being automatically processed’.[34] The CJEU has ruled in a case called *Lindqvist* that if data was located on a European server and accessed from outside the EU, that would not constitute a data transfer for the purposes of EU data protection law.[35] Kuner does not think that this decision is very helpful in defining a data transfer since the decision was based on certain technical factors and speculates that the decision was at least partly affected by the facts in question and considering that it was small scale. A company handling large amount of data online would more likely fall within the data transfer definition.[36]

However, it is to be noted that in the context of the internet it is not always clear that the transfer has taken place at all, since the data could still be physically located on a European server, but only accessed from the United States. In fact, data transfer is rather an ongoing process.[37] According to Gonzáles Fuster it is not really the movement or flow of data which is in question,

[31] Article 2, Data Protection Directive.
[32] Art. 4(1), General Data Protection Regulation.
[33] § 1(c), OECD Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013).
[34] Article 12(1), Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981 (Convention 108).
[35] Case C-101/01, Bodil Lindqvist, paras 60–61, 68 and 70.
[36] Kuner, (2007), p. 81–83.
[37] Kuner, (2013), p. 11.

but rather just different data processing activities which may raise questions of conflict of laws.[38] However, considerations whether data transfer has taken place are outside the scope of this research, the focus is on situations where it has taken place and there has been a breach of some kind.

I already mentioned above what I mean by 'redress', but for the purposes of this study it is necessary to clearly define what is meant by it. Oxford English Dictionary defines it as 'reparation or compensation for a wrong or consequent loss' and 'remedy for or relief from trouble'.[39] This is what I also mean by 'redress'. Thus some sort of compensation or damages awarded to repair the loss suffered as a result of data protection rules being breached. These could be monetary compensations or something else. The Privacy Shield, which is the focus of this study, offers a range of non-monetary compensations, such as correction or deleting the personal data. Redress mechanism is then a way to seek this redress. Usually redress is sought through judicial means, but as will be seen there are also other ways.

Still useful to note are terms 'data processor' and 'data controller'. 'Data processor' is an organisation that processes personal data. There are multiple ways the processing could take place.[40] 'Controller' on the other hand determines the means and purposes of the processing.[41] Both could be legal or natural persons.

1.4. Methodology

Multiple methods are used in this research. Firstly, doctrinal law research is used. Doctrinal law research studies legal texts and how to interpret them.[42] The research is going to look into the legal documents relating to data protection, most importantly the official documents of the Safe Harbour and the Privacy Shield. EU data protection legislation will also be discussed, particular secondary legislation, such as the Data Protection Directive of 1995, which is the legal basis for the Safe Harbour Decision. Additionally the thesis will also look into the new General Data Protection Regulation (GDPR) and what changes it will bring to the field of data

[38] González Fuster, (2016), p. 162.
[39] Oxford English Dictionary online.
[40] See Art. 2(b) and (e), Data Protection Directive and Art. 4(2) and (8), General Data Protection Regulation.
[41] Art. 2(d), Data Protection Directive and Art. 4(7), General Data Protection Regulation.
[42] Hirvonen, (2011), p. 36.

transfers and redress mechanisms. Also important are the Charter of Fundamental Rights and European Convention on Human Rights.

This research is done from a European perspective, hence detailed analysis of US law is outside the scope of this thesis. Additionally study and analysis of case law will be included. Most importantly the case law of the Court of Justice of the European Union (CJEU), the most important case for this study is the *Schrems* case, but I shall also be looking into other cases in order to determine the status of data protection in the EU and also define what effective redress is in the European case law. Some cases from the European Court of Human Rights (ECtHR) are also be included in the research because they help in determining the status and extent of the European right to data protection and also the right to seek redress (or effective remedy).

Comparative Law method is also used to compare the redress mechanism of the Safe Harbour and the Privacy Shield. In the academic field there is some disagreement as to what is meant by comparative law method and as to how objective it can be.[43] In this study, however, comparative law methods means a simple comparison, i.e. I am looking at two different objects and seeing what is different and similar between them.

Additionally some law in policy oriented discussion will be included. As data protection often has to be reconciled against other interests, such as economic, I shall be discussing this tension between these two interests. Legal research has often used other disciplines, such as sociology or economics, to look at law from a different perspective.[44] However, I shall not be using law and economics type of method, as I am not directly interested in the economic effects of the Privacy Shield, but rather only the tension between data protection and the economic interest of data.

This thesis also covers multiple fields of law. European law is at the centre point, but also information law, comparative law, procedural law and private international law are used. I shall asses the Safe Harbour and more importantly the Privacy Shield by using Europeans law, most importantly the case law of the CJEU. Data protection itself encompasses multiple areas of law. It has become part of European law, but perhaps most obviously it is part of information law. Since the focus is on the ability of EU citizens to seek redress through (non-)judicial means this study thus also encompasses procedural law. Finally, since the jurisdictional conflict between

[43] Glanert, (2012), pp. 61–70.
[44] Hirvonen, (2011), p. 28.

the EU and the US in matter of data protection is discussed, the thesis does also touch on the law of conflicts, i.e. private international law.

1.5. Structure of the Thesis

In Chapter 2 the background and objectives of European data protection law will be discussed. I shall focus specifically why such Adequacy Decisions, such as the Safe Harbour and the Privacy Shield are needed. In that Chapter I shall also analyse the Safe Harbour Decision and more specifically the redress mechanism that were offered in that regime. I will also discuss the famous *Schrems* case that lead to the invalidation of the Safe Harbour. I will discuss the weaknesses of the Safe Harbour and analyse why it failed and also introduce the criteria that the CJEU established to assess Adequacy Decisions. The following Chapter 3 shall then discuss the Privacy Shield Decision and most importantly the redress mechanisms of that regime. This study will find that there has been some significant changes in terms of redress mechanisms offered, the Privacy Shield has introduced new options to seek redress. However, the main focus of this thesis is to assess the Privacy Shield redress mechanisms. In Chapter 4 I shall assess the redress mechanisms using the CJEU criteria that was established in the *Schrems* case. I will review them by using European case law, both CJEU case law and also ECtHR case law, to determine whether the Privacy Shield would pass the *Schrems* criteria. The research shall find that the new redress mechanisms do not fulfil all the requirements, despite there has been notable improvements. In the final Chapter I will then discuss more specifically, why I think that the Privacy Shield would not pass the CJEU criteria on part of the redress mechanisms. I shall also briefly discuss the tension between data protection and the economic objective of data protection legislation. I shall also review some suggestions that have been introduced to solve the problems with the Privacy Shield redress mechanisms and introduce my own ideas.

2. Background to the Study: EU Data Protection Law and the Safe Harbour

2.1. EU Data Protection Law

Before going ahead for the main topic of comparing the Safe Harbour and the Privacy Shield, it is useful first take a look at data protection law in the European Union and more specifically why such a regime as the Safe Harbour or the Privacy Shield is required for transatlantic data transfers. A brief overview of the main legislation and the objectives of EU data protection legislation is required at this point. In this part I shall firstly briefly explain how data protection became part of Union legislation and eventually became a fundamental right. Secondly, I shall look at secondary legislation, which relates to data protection. And thirdly, I will discuss Adequacy Decisions.

2.1.1. Objectives and Fundamental Rights

The basis for EU data protection legislation is found not only in fundamental right considerations but also concerns about the functioning of the internal market. A detailed analysis of the emergence of EU data protection law is outside the scope of this research, but at this point it is necessary to note that the emergence of European data protection legislation has from the beginning been coloured by both human rights and internal market considerations. The development of EU data protection law was also influenced by 1980 Organisation for Economic Co-operation and Development (OECD) Guidelines[45] and Convention 108[46], which both stressed the importance of both protecting privacy while simultaneously ensuring free flow of information.[47] In fact the internal market considerations were more important in the beginning since the EU was early considered to be more of an economic union than a protector of human rights. It was considered that data protection was necessary for the functioning of the internal market

[45] See Preface, OECD Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (23 September 1980).
[46] Preamble, (Convention 108).
[47] González Fuster, (2014), p. 111–122.

and the actualisation of the four freedoms. Free flow of personal data was necessary for the European Union.

According to Article 5 of the Treaty on the European Union, the principle of subsidiarity applies to Union decision making.[48] The competences of the Union are based on the principle of conferral and actions which do not fall exclusively within the Union competence, the Union may act only if it is considered that the objectives cannot be sufficiently achieved by Member state acting independently. Hence the objectives are better achieved by collective Union action rather than Member States acting individually. This was the case for data protection and how it became to fall within the Union competences. Union interest in data protection started already in the 1970s when there started to be concerns of US dominance in the area and perhaps more importantly the fear of divergent laws across the Union. Data protection was deemed to be of constitutional importance to the Union.[49]

Data protection has also been included in the EU treaties. Relevant provision in the Treaties, are Article 39 TEU[50] and Article 16 TFEU[51], which relate to the EU competence in data protection issues. For the purposes of this study, however, more important is Article 8 of the Charter of Fundamental Rights[52], according to which data protection is a fundamental right. Data protection was in the end included as separate provision to privacy, even though there had been discussion whether it was in fact separate.[53] The Charter became legally binding and equivalent with the EU Treaties with the entry into force of the Treaty of Lisbon in 2009.[54] According to Article 6(1) of the TEU, it has same value as the Treaties.[55] Hence, not only is protection of personal data recognized as a fundamental right, the data protection legislation of the EU has from the beginning also had the objective of ensuring the free flow of data.

[48] Article 5, Treaty on the European Union.
[49] González Fuster, (2014), p. 112.
[50] Art. 39, Treaty in the European Union. Under this provision the Council has the authority to lay down rules relating to data protection when the activities fall within the scope of Chapter 2 of the TEU.
[51] Art. 16, Treaty on the Functioning of the European Union. Under Art. 16(1) everyone has the right of data protection and under Art. 16(2) the European Parliament and the Council can lay down rules relating to data protection with regard to processing by EU institutions and Member States when they are doing activities that fall within the scope of EU law, as well as rules relating to free movement of personal data.
[52] Art. 8, The Charter of Fundamental Rights.
[53] González Fuster, (2014), pp. 195–198.
[54] EU Charter of Fundamental Rights, website of the European Commission.
[55] Art. 6(1), Treaty on the European Union.

2.1.2. Data Protection in Secondary Legislation of the EU

The central pieces of legislation are Directive 95/46/EC more commonly known as the Data Protection Directive (Hereinafter referred to as the Data Protection Directive or the DPD)[56] and Regulation (EU) 2016/679, or the General Data Protection Regulation (hereinafter referred to as the GDPR).[57] EU data protection law is going through a reform and a new piece of legislation, the GDPR shall replace the Data Protection Directive. It is going to become fully applicable in May 2018.[58]

First of all the DPD, the name of the Directive 'on the protection of individuals with regard to the processing of personal data and on the free movement of such data' already reveals its purpose, it is meant to protect individuals with regard to processing of personal data and on the other hand it is meant to 'protect' free movement of data. These same objectives are also stated in Article 1 of the Directive. Recitals 1–6 of the Preamble also state that economic integration and the internal market require the free flow of data across Member States and recitals 8 and 9 of the Preamble speak of the need to harmonize data protection laws across the Union.[59] When the DPD was adopted there were both internal market considerations relating to free movement and also the concern for the need to ensure the right to privacy which was understood as a general principle of Union law.[60] Secondly the GDPR echoes the same two objectives of ensuring protection of natural persons with regard to processing of personal data while simultaneously ensuring the free flow of such data.[61] These two pieces of legislation thus further emphasize the importance of the dual objectives of the EU data protection legislation.

2.1.3. Adequacy Decisions

I already mentioned in Chapter 1 that transferring personal data to third countries, such as the US, is only possible if the data protection in that third country in question is adequate. The legal basis for this is found in the DPD. Article 25 paragraphs 1 and 2 state:

[56] Directive 95/46/EC, (Data Protection Directive).
[57] Regulation (EU) 2016/679, (General Data Protection Regulation).
[58] GDPR website.
[59] Preamble recitals 1–6, 8 and 9, Data Protection Directive.
[60] González Fuster, (2014), p. 126.
[61] See paras. 2 and 3 of the Preamble and Art. 1, General Data Protection Regulation.

> 1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.
>
> 2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.[62]

The European Commission was given the power to decide on the adequacy of a given third state by the Council and the European Parliament.[63] In this study, these decisions are called 'Adequacy Decisions'.[64] The Commission can make a decision as to the adequacy of the data protection laws of a certain third country on the basis Article 25 (6) of the DPD which states:

> 6. The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.[65]

The exact procedure of determining adequacy is not relevant here. It suffices to note what the Commission needs to consider. Article 25 (2) of the DPD states that 'all the circumstances' have to be taken into account. The Article 29 Working Party[66] (WP29) had laid down some

[62] Article 25(1) and (2), Data Protection Directive.
[63] Commission decisions on the adequacy of the protection of personal data in third countries, Website of the European Commission.
[64] However Adequacy Decisions are not the only means of transferring data to third countries. Under Article 26(2), Data protection Directive, transfers are allowed where there are 'appropriate contractual clauses'. These can be either Model Contractual Clauses (MCCs) or Binding Corporate Rules (BCRs).
[65] Article 25(6), Data Protection Directive.
[66] Article 29 Working Party is a body created by the Data Protection Directive to work as an independent advisor in the field of data protection. Even though the body cannot make binding decisions, the advisory opinions

guidelines as to what are the factors that need to be taken into account. The most interesting ones out of those for the purposes of this research are procedural and enforcement mechanisms, which in particular ought to include good level of compliance first of all, support and help to the individual in the exercise of the their rights and lastly appropriate redress in case of injuries.[67]

Under the new regulation (GDPR) which is about to replace the Data Protection Directive there is a similar provision granting the Commission the power to make an Adequacy Decision, Article 45.[68] It is more detailed, specifically paying attention to human rights and rule of law, effectiveness of supervisory authority and commitments made by the third country in question in relation to data protection.[69] As with the DPD Article 25 (1), according to Article 45 (1) of the GDPR transfers are allowed only when the third country ensures adequate level of protection.[70]

Similarly as under the DPD rules, the Commission can make a decision about the adequate level of data protection in the country in question, according to Article 45 (3) of the Regulation.[71] The provision introduces two significant changes. First of all, the GDPR codifies that the Adequacy Decisions may be limited to a territory or a specific sector. Additionally periodic reviews of adequacy are required. However, as regards to what need to be taken into consideration in determining the adequacy of the level of data protection in a given country, the GDPR introduces a very detailed provision. According to Article 45 (2) the Commission must in particular pay attention to 'respect of human rights and fundamental freedoms', 'effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred' as well as enforcement issues amongst other things.[72]

---

of the Working Party have significance. It works as sort of a mediator between Member States and the Commission bringing the opinions about data protection from the state level to the Commission as well as promoting uniform application of the DPD principles at state level, advising the Commission about data protection issues and issuing recommendations. Article 29 and 30, Data Protection Directive. See also the website of the European Data Protection Supervisor, and also Article 29 Data Protection Working Party tasks. See also Article 1, Article 29 Working Party Rules of Procedure.

[67] WP29 Working Document, (1998), p. 6–7.

[68] Article 45, General Data Protection Regulation.

[69] Bräutigam, (2016), p. 148.

[70] Article 45(1), General Data Protection Regulation.

[71] Article 45(3), General Data Protection Regulation.

[72] Article 45(2), General Data Protection Regulation.

The changes in the legislation will be relevant to my analysis of the redress mechanisms of the Privacy Shield, as the CJEU would potentially take the new regulations into consideration if it were to assess the Privacy Shield.

2.2. Rise and Fall of the Safe Harbour

In this part I will briefly summarize what the Safe Harbour was and what where the redress mechanisms under that regime. Then I shall review the CJEU case, where the Safe Harbour was invalidated, and the criteria for assessing Adequacy Decisions was established.

2.2.1. Safe Harbour Decision

The Safe Harbour was an Adequacy Decision that the Commission made according to Article 25(6) of the DPD[73] to comply with the requirement of adequate data protection as required in Article 25(1) in that same Directive.[74] Under that regime data could be transferred from the EU to the US. The Commission passed the decision 2000/520/EC in July 2000 (hereinafter referred to as the Safe Harbour Decision).[75]

The differences between the US and EU approach to data protection was one of the main reasons for the Safe Harbour decision, to ensure the flow of data across the Atlantic and promote commerce. As already described in Chapter 1 the US approach to data protection in fundamentally different and Adequacy Decision is a way to solve this problem. Engagement in transatlantic commerce, from the perspective of the EU, is a threat to data protection, or at least how it is understood in the EU. In cross-border situations, conflict of law may materialize and par-

[73] Art. 25(6), Data Protection Directive.
[74] Art. 25(1), Data Protection Directive.
[75] 2000/520/EC, 'The Safe Harbour Decision'.

ticularly in data protection issues questions of jurisdiction and enforcement are unclear. Therefore cooperation between the EU and the US in data protection issues is a way of circumventing these hurdles.[76]

Thus the Safe Harbour was basically a framework under which US organizations (private companies or public organisations) could transfer personal data of EU citizens to the US while still complying with the EU data protection laws.[77] The regime was self-certifying, US companies wishing to participate had to inform the US Department of Commerce (hereinafter referred to as DoC) that they would adhere with the Safe Harbour rules.[78] The Safe Harbour regime was an 'extraordinary' Adequacy Decision in the sense that it did not make all transfers of personal data from the EU to the US possible and thus 'deciding' that US has adequate level of data protection. Rather, since the US did not have adequate data protection, the Safe Harbour offered an optional set of rules that organisations could voluntarily adhere to satisfy with the adequacy requirement of EU law. Thus the Safe Harbour was a 'partial' Adequacy Decision, only certain type of transfers were allowed.[79]

The Safe Harbour was in many ways a compromise. There was a need to ensure the free flow of data at the both sides of the Atlantic, but then there was the problem that European law did not allow data transfers unless the destination country offered adequate protection, and the US sectoral self-regulating system did not meet the European requirements. Nor was there any political will in the US to change the law. There was the danger of potential enforcement actions in Europe and showdown judgement in the US, the Safe Harbour offered a way to delay these potential threats.[80]

[76] DiLascio, (2004), p. 400.
[77] Rotenberg and Jacobs, (2013), p. 638.
[78] Khan, Part 1, (2016), p. 3. See also 'The Safe Harbour Decision', Annex II, Frequently Asked Questions (FAQs), FAQ 6.
[79] Kuner, (2007), p. 175.
[80] Reidenberg, (2001-2002), p. 739–740.

2.2.2. Structure of the Safe Harbour and Redress Mechanisms

The Safe Harbour Decision contained a set of Safe Harbour Privacy Principles ('Principles') and a set of Frequently Asked Questions ('FAQs'), included in Annexes I and II respectively.[81] The purpose of the Principles was to ensure that the US organisations collecting and processing EU citizens personal data would do so in a way that would be deemed adequate from the EU perspective and thus facilitating commerce between the EU and the US.[82] To qualify those organisations had to apply the Principles for transfers of personal data of EU citizens across the Atlantic.[83] The FAQs, on the other hand, were meant to be more specific guidance as to how to apply the Principles.[84] Here only the Principles and FAQs which relate to EU citizens redress opportunities will be discussed.

The Safe Harbour had seven data processing principles that US companies had to comply with. Those were Notice, Choice, Onward Transfer, Security, Data Integrity, Access and Enforcement.[85] From these the Enforcement Principle is obviously the most relevant, although it cannot be said that any of the seven principles would be irrelevant, since failure to comply with any of the Principles would have potentially amounted to a breach thus giving rise to action for redress. However, since the focus is on the redress mechanisms, only the Enforcement Principle shall be discussed.

Hence, the Enforcement Principle of the Safe Harbour stated:

> Effective privacy protection must include mechanisms for assuring compliance with the Principles, recourse for individuals to whom the data relate affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed. At a minimum, such mechanisms must include
>
> (a) readily available and affordable independent recourse mechanisms by which each individual's complaints and disputes are investigated and resolved by reference to the Principles and damages awarded where the applicable law or private sector initiatives so provide;
>
> (b) follow up procedures for verifying that the attestations and assertions businesses make about their privacy practices are true and that privacy practices have been implemented as presented; and

[81] US law applied to questions of interpretation and compliance with the Principles and Frequently Asked Questions. See 'The Safe Harbour Decision', Annex I, Safe Habor Privacy Principles, para. 6. The advantage of this was that US companies were likely to be comfortable with their own domestic law. See Kuner, (2007), p. 182–183.
[82] 'The Safe Harbour Decision', Annex I, Safe Harbor Privacy Principles, para 2.
[83] 'The Safe Harbour Decision', Annex I, Safe Harbor Privacy Principles, para 5.
[84] 'The Safe Harbour Decision', Art. 1.
[85] 'The Safe Harbour Decision', Annex I, Safe Habor Privacy Principles. See also: Kuner, (2007), p. 187.

> (c) obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations.[86]

Thus in practice, the Safe Harbour imposed three requirements to ensure compliance, (a) readily available and affordable independent recourse mechanisms, (b) follow up procedures and (c) an obligation to remedy problems. More specific instructions as to how to comply with these requirements were found in the FAQs, which are analysed next.

The Safe Harbour Decision included fifteen FAQs in total. Only the ones that relate to the redress mechanism available for individual data subject are discussed here. The most relevant ones were FAQ 5 (The Role of the Data Protection Authorities), FAQ 6 (Self-Certification), FAQ 7 (Verification) and finally FAQ 11 (Dispute Resolution and Enforcement).

First of all, FAQ 6 that relates to self-certification. The US organisation that wished to adhere to the Safe Harbour Principles had to self-certify, in other words, to register with the US DoC, with some information about the organization which included, *inter alia* detail of the company's privacy policy. It had to contain such information as where individuals would find information about the privacy policy, contact for case of complaints and requests, a statutory body that had jurisdiction to hear claims, potential privacy programmes that the organisation is a member of, method of verification and independent resource mechanism.[87] Thus when the company wanted to register with the Safe Harbour regime it had to provide information how and where and individual data subject could make complaints. US organisations had the choice between different dispute resolution options under the Safe Harbour regime.

FAQ 11 relating to dispute resolution and enforcement explained in more detail of the options that US organisations had. FAQ 11 addresses requirement (a) and (c) of the Enforcement Principle, thus the requirements of readily available and affordable recourse mechanisms and the obligation to remedy problems. To meet the second requirement (b) follow up procedures, companies that wished to qualify with the Safe Harbour had to act according to FAQ 7 (Verification), thus verify through self-assessment or outside compliance reviews. Under both of these options, the company ensures, either through self-assessment or an external body, that an individual is well informed about the ways to complain and how to pursue recourse mechanisms and that the mechanism and procedures are effective in place.[88] To satisfy requirements (a) and

[86] 'The Safe Harbour Decision', Annex I, Safe Habor Privacy Principles, Enforcement.
[87] 'The Safe Harbour Decision', Annex II, Frequently Asked Questions (FAQs), FAQ 6.
[88] 'The Safe Harbour Decision', Annex II, Frequently Asked Questions (FAQs), FAQ 7 and FAQ 11.

(c), recourse mechanisms and remedies there were options but the organisations were free to choose as long as they would meet the requirements set out in the Enforcement Principle. FAQ 11 listed some examples of the mechanisms that companies could use to satisfy with the requirements:

> (1) compliance with private sector developed privacy programs that incorporate the Safe Harbor Principles into their rules and that include effective enforcement mechanisms of the type described in the Enforcement Principle;
>
> (2) compliance with legal or regulatory supervisory authorities that provide for handling of individual complaints and dispute resolution; or
>
> (3) commitment to cooperate with data protection authorities located in the European Union or their authorized representatives[89]

FAQ 11 also set out some more specific instructions: firstly individuals ought to be encouraged to raise complaints with the relevant organisation before relying on other recourse mechanisms. The dispute resolution body had to investigate all complaints unless they were completely unfounded or frivolous. There had to be full and readily available information about the options the individual had if she or he wanted to file a complaint. Secondly, remedies had to reverse or correct the effect of non-compliance with the Principles, the organisation had to comply with the Principles in the future and where appropriate the future processing of the personal data of the individual data subject in question had to end. Sanctions had to have the effect of ensuring compliance with the Principles, which could mean, when appropriate, removal of the seal. When the dispute was heard by a private dispute resolution body, the DoC and the governmental body with the applicable jurisdiction had to be notified about the failure of the organisation to comply with the Principles. Thirdly, the Federal Trade Commission[90] (hereinafter referred to as the FTC) would review regularly referrals from independent self-regulatory organisation.

[89] 'The Safe Harbour Decision', Annex II, Frequently Asked Questions (FAQs), FAQ 11.

[90] The FTC or the Federal Trade Commission is an independent US government body that has powers to hear claims and seek redress or other relief to consumers whose right have been violated under section 5 of the Federal Trade Commission Act. See Federal Trade Commission Act, Incorporating U.S. SAFE WEB Act amendments of 2006, Sec. 5.

Finally, persistent failure to comply with the Principles would result that the organisation in question would no longer be able to participate in the Safe Harbour regime.[91]

If a US organisation had chosen to comply with the European Data Protection Authorities[92] (hereinafter referred to as DPAs), FAQ 5 applied. According to FAQ 5 US organisations had to cooperate in matters of investigation and resolution of complaints and remedial and compensatory measures. In practice, cooperation happened through advice given by an informal panel at the European level DPA. The purpose of the advice was to ensure that Principles are followed and remedies are given when appropriate. The informal panel would give advice in situations where complaints were referred to it from the US organisation or were individuals would complain to the DPA directly. The DPA would also direct individuals to make an in-house complaint at the first instance. Both sides had to be heard by the DPA and there had to be an opportunity to make comments or produce evidence. In case of failure to comply with the DPA advice, the DPA could notify the FTC or another US body with powers to take enforcement action. Alternatively, the DPA could conclude that the agreement to cooperate with the Safe Harbour is null and void and notify the Department of Commerce to amend the list of participants.[93]

Summa summarum, an individual data subject in the EU had choices where to seek redress under the Safe Harbour regime. In no particular order the first option was a direct complaint to the relevant US organization. Secondly, individual could complain to the self-regulatory supervisory authority that could be located in the US or the EU, if the organization in question had chosen this method of dispute resolution. Examples of those would be BBBOnline and TRUSTe. Thirdly, complaints could be made to legal or regulatory supervisory authorities, again if the US organization had chosen that method. According to the Safe Harbour Decision, two US government bodies were able to investigate complaints and redress, the FTC and the Department of Transportation.[94] And fourthly, if the organization had chosen the option to cooperate with European Data Protection Authorities, a complaint could be forwarded to such a body. The self-regulatory supervisory authority or the DPA could also forward the matter to the FTC of the DoC.[95] It ought to be noted that potentially there could have been other routes to pursue recourse, since the Safe Harbour Decision was not exhaustive in its listing of ways to

[91] 'The Safe Harbour Decision', Annex II, Frequently Asked Questions (FAQs), FAQ 11.
[92] These are national data protection authorities. There is a DPA in all EU countries. For a list of national DPAs see Data Protection Authorities list.
[93] 'The Safe Harbour Decision', Annex II, Frequently Asked Questions (FAQs), FAQ 5.
[94] 'The Safe Harbour Decision', Annex.
[95] 'The Safe Harbour Decision', Annex II, Frequently Asked Questions (FAQs), FAQ 5 and FAQ 11.

ensure enforcement. These four, however, would have been the most obvious and perhaps suitable for an individual data subject.

It is noteworthy that the abovementioned methods are all non-judicial. In other words the Safe Harbour only offered means to seek redress through Alternative Dispute Resolution (ADR).[96] The Safe Harbour Decision was thus not clear whether court action in the US was possible. And even if it was possible, it would have been difficult and inconvenient also because US law took supremacy.[97]

2.2.3. Deficiencies with Safe Harbour Redress Mechanisms

Despite the options listed above seem to offer multiple options, the regime was still unsatisfactory in many respects. Two major weaknesses were that it was voluntary and self-certifying.[98] Qualification with the Safe Harbour was voluntary and there were different ways to qualify. For instance an organization could join a self-regulatory privacy program or develop their own privacy policy.[99] To qualify an organization had to thus comply with the Principles and publicly declare that it does so. Some studies also suggested that compliance with the regime was somewhat alarming.[100] According to Kuner the main problems with the Safe Harbour were the lack of compliance with the Principles and the small number of complaints brought against it. Since it was difficult to assess the regime without any dispute brought in front of a judge.[101] Problem was also the informational asymmetry, in other words, the lack of knowledge of the data subjects about the data protection practices and redress options available to them.[102]

At the time when the Safe Harbour was still being drafted, the Article 29 Working Party raised some concerns about the Enforcement principle. The relationship between Alternative Dispute Resolution and the Federal Trade Commission was uncertain. The dispute resolution body chosen by the US organisation (self-regulatory supervisory authority, DPA or some other) had no

[96] Alternative Dispute Resolution is any dispute settlement that happens outside the courtroom. See e.g. Legal Information Institute website.
[97] DiLascio, (2004), pp. 422–423.
[98] Markel, (2006), p. 2.
[99] 'The Safe Harbour Decision', Annex I, Safe Habor Privacy Principles, para. 3.
[100] Markel, (2006), pp. 7–10.
[101] Kuner, (2007), p. 191.
[102] Mouzakiti, (2015), p. 43.

obligation to inform the FTC about breaches and there were no guarantees that the FTC would examine the case if an individual complained directly to the FTC.[103]

Also there was a problem with the FTC enforcement. The powers of enforcement on the US side were referred to the Federal Trade Commission (FTC) under section 5 of the Federal Trade Commission Act. The legal authority of the FTC is questionable as regards to the enforcement of the Safe Harbour, because it does not match the US Supreme Court's interpretation of Section 5 authority.[104] The 29 Working Party had also noted that certain sectors, such as telecommunications, transportation or employment, fell outside the scope of FTC powers.[105] Only organisations that fell within the jurisdiction of the FTC could participate.[106]

Remedies were another issue. According to Articles 23 and 24 of the DPD data subjects must be afforded compensation and the violating organisation must be sanctioned,[107] but there were concerns that the Safe Harbour did not offer sufficient standard of redress consistent with Article 22 and 23 the Data Protection Directive.[108] The DoC had assured that remedies would be provided.[109] The problem was that these actions had not been established in US courts.[110]

The greatest flaw, however, was that these redress avenues were limited to commercial disputes and actions against public US bodies were not possible under the Safe Harbour. The CJEU also noted in the *Schrems* case that the Safe Harbour did not contain any means for individual data subjects to seek redress against the action of US public authorities.[111] FTC jurisdiction also does not extend to other than commercial disputes.[112] Similarly private dispute resolution bodies, such as BBBOnline or TRUSTe, do not have authority to decide on the lawfulness of US security agencies.[113] Hence, under the Safe Harbour there was not any opportunity to bring a claim against the actions of US public bodies. As will be seen in the next section, where I shall discuss

[103] WP29 Opinion 4/2000, p. 7.
[104] Reidenberg, (2001-2002), p. 740–741.
[105] WP29 Opinion 4/2000, p. 4.
[106] DiLascio, (2004), p. 415.
[107] Arts. 23 and 24, Data Protection Directive.
[108] Reidenberg, (2001-2002), p. 744–745.
[109] Department of Commerce Memorandum.
[110] Reidenberg, (2001-2002), p. 745.
[111] Case C‑362/14, *Schrems* case, para. 90.
[112] 'The Safe Harbour Decision', Annex II, Frequently Asked Questions (FAQs), FAQ 11, FTC Action. And Annex III, Annex V and Annex VII.
[113] Opinion of Advocate General Bot, Case C‑362/14, Maximillian Schrems v Data Protection Commissioner, para. 206.

the *Schrems* case, Max Schrems managed to indirectly challenge the surveillance activities of US public authorities by bringing a case in the EU.

2.2.4. The *Schrems* case and the Invalidation of the Safe Habour

The famous *Schrems* case, which perhaps surprisingly to some managed to knock down the Safe Harbour, was initiated by an Austrian law student Maximillian Schrems who complained to the Irish Data Protection Commissioner to prevent Facebook Ireland from transferring his personal data to the United States.[114] In this part the *Schrems* case will be summarized and analysed. In the following part I will discuss the criteria that the CJEU established in this *Schrems* case to assess Adequacy Decision. Some flaws and weaknesses of the Safe Harbour have already been shown above, thus here the focus will be on the CJEU decision of the *Schrems* case.

Facebook Inc., a US company has a European subsidiary, Facebook Ireland. EU citizen wishing to register with Facebook need to have a contract with Facebook Ireland, allowing them to transfer their personal data to Facebook Inc. in the United states, where the data is processed.[115] Max Schrems filed a complaint soon after the so called Snowden revelations because he considered that the US did not provide adequate level of data protection as it was required by EU law, his argument was that the revelations of Edward Snowden proved that the United States did not have meaningful data protection.[116] The Irish Data Protection Commissioner rejected the complaint considering that since there was no evidence of Schrems's personal data being accessed by the NSA[117] and also it considered that the Commission had decided in the Safe Harbour Decision that the United States had adequate level of data protection, there was no need to investigate the matter further.[118] Schrems proceeded to take the case to the Irish High Court that considered that despite the Data Protection Commissioner was bound by the Safe Harbour Decision, considering the entry into force of Article 8 of the Charter of Fundamental

[114] Case C‑362/14, *Schrems* case para. 28.
[115] Case C‑362/14, *Schrems* case, para. 27.
[116] Maximillian Schrems v Data Protection Commissioner, [2013 No. 765JR], [2014], IEHC 310, para. 29.
[117] National Security Agency. A US intelligence organization. See NSA website.
[118] Case C‑362/14, *Schrems* case, paras. 28–29. See also Maximillian Schrems v Data Protection Commissioner, [2013 No. 765JR], [2014], IEHC 310, paras. 30–33.

Rights, the application of Schrems essentially raised question of European law and the Court decided to refer questions to the CJEU.[119]

The questions referred to the CJEU essentially asked whether the Irish Data Protection Commissioner was bound by the Safe Harbour Decision also having regard to Article 7, 8 and 47 of the Charter[120] and Article 25(6) of the DPD[121] and thus also preventing examination of a claim from an individual data subject. And alternatively whether the Data Protection Commissioner may conduct its own investigations of the matter.[122] In the Court's decision two particular points were discussed, the competence of the DPAs to assess the claim and the validity of the Safe Harbour decision.

The first point does not have to be discussed in detail. What is relevant for the purposes of this study is that the Court decided that in the light of Article 8(1) and (3) of the Charter[123] national authorities must be able to investigate independently whether the data transfer complies with EU data protection rules even if there is a Adequacy Decision by the Commission in place.[124] The court endorsed the Opinion of AG Bot, who considered that DPAs must be able to hear claims because of their role as guardians of human rights and also the Commission did not have exclusive powers to decide on the adequacy, and deprivation of investigative powers would be contrary to the purpose of the Data Protection Directive.[125]

Secondly, the validity of the Safe Harbour Decision was being questioned. The CJEU stated that it was the only body that had the authority to decide on the validity of such EU act.[126] The Court did indeed decide that the Safe Harbour Decision was invalid. It considered that the data protection rules of the Data Protection Directive could be easily circumvented unless the third country in question had 'essentially equivalent' level of data protection, thus moving slightly from the 'adequate' level of data protection. The Court followed the Opinion of AG Bot, who thought that the objective of the DPD was essentially 'to ensure the continuity of the protection

[119] Maximillian Schrems v Data Protection Commissioner, [2013 No. 765JR], [2014], IEHC 310, paras. 64–70.
[120] Arts. 7, 8, 47, Charter of Fundamental Rights.
[121] Art 25(6) Directive 95/46/EC, Data Protection Directive.
[122] Case C‑362/14, *Schrems* case, paras. 36–37.
[123] Art. 8(1) and (8(3), Charter of Fundamental Rights.
[124] Case C‑362/14, *Schrems* case, paras. 57–58. Even though the Adequacy Decision is binding to the DPAs, they must still be able to investigate claims by individuals. See Case C‑362/14, Maximillian Schrems v Data Protection Commissioner, joined party: Digital Rights Ireland Ltd, paras. 28–29.
[125] Opinion of Advocate General Bot, Case C‑362/14, Maximillian Schrems v Data Protection Commissioner, paras. 61, 73, 92, 93, 95.
[126] Case C‑362/14, *Schrems* case, paras. 61–62.

afforded by that directive'.[127] And, as was required by Article 25 (2) of the DPD[128], all the circumstances governing the transfer of personal data had to be taken into account and hence also subsequent events that have arisen since the adoption of the Safe Harbour Decision and to be considered when determining the adequacy level of data protection in a third country. [129]

According to Article 25 (6) of the DPD[130] the Commission must guarantee that United States 'ensures an adequate level of protection'…'by reason of its domestic law or of the international commitments'…'for the protection of the private lives and basic freedoms and rights of individuals'. The Court considered that the Safe Harbour did not guarantee this because 'national security, public interest and law enforcement requirements' took primacy over Safe Harbour Principles.[131] Moreover, individuals had no means of redress against interferences of that kind since disputes before the FTC were limited to commercial disputes.[132] EU citizens also do not have effective right to be heard in the United States in disputes like this.[133] The lack of effective judicial review was against Article 47 of the Charter.[134] AG Bot also noted that the inability to bring disputes against public bodies meant that personal data is not effectively protected.[135] Furthermore the Court considered the national data protection supervisor's ability to assess claims by individuals and stated that Article 28 of the DPD[136] read in conjunction with the Article 8 of the Charter[137] means that they must be able to do so. Article 3(1) of the Safe Harbour Decision restricted this right and the Commission had exceeded its powers when adopting that provision.[138] The Court's finding was, that Article 1 of the Safe Harbour Decision did not ensure

[127] Opinion of Advocate General Bot, Case C-362/14, Maximillian Schrems v Data Protection Commissioner, paras. 139–141.
[128] Art. 25(2), Data Protection Directive.
[129] Case C-362/14, *Schrems* case, paras. 73–78.
[130] Art. 25(6), Data Protection Directive.
[131] Case C-362/14, *Schrems* case, paras. 79–86.
[132] Case C-362/14, *Schrems* case, paras. 89–90. AG Bot also noted this. See Opinion of Advocate General Bot, Maximillian Schrems v Data Protection Commissioner, para. 165.
[133] Opinion of Advocate General Bot, Case C-362/14, Maximillian Schrems v Data Protection Commissioner, para. 173.
[134] Case C-362/14, *Schrems* case, para. 95. See also Art. 47, Charter of Fundamental Rights.
[135] Opinion of Advocate General Bot, Case C-362/14, Maximillian Schrems v Data Protection Commissioner, para. 207.
[136] Art. 28, Data Protection Directive. The provision regulates the powers of supervisory authorities. It states, *inter alia*, that they must be independent and have investigative powers.
[137] Art. 8, Charter of Fundamental Rights.
[138] Case C-362/14, *Schrems* case, paras. 99–104.

adequacy and also Article 3 of the Decision exceeded the powers of the Commission, and with those flaws, the Safe Harbour was found invalid.[139]

The Safe Harbour fell short of essentially four main things. First, there was a lack of effective control mechanism for the self-certification regime. Second, US law prevailed, which meant that national security or public interest could prevail over data protection safeguards. Third, there were deficiencies in the Safe Harbour Decision itself. And finally, access by US authorities to personal data of EU citizens violated fundamental rights.[140] Bräutigam calls the decision 'the culmination of European uneasiness with U.S. national security law.'[141] I would agree with this as the assessment of the Court was largely affected by mass surveillance and most probably the recent Snowden revelations had an influence. As regards to redress mechanism I agree with the Court that the Safe Harbour was unsatisfactory, especially since it did not offer any means of bringing claims against US public authorities.

2.2.5. Criteria for Assessing an Adequacy Decision

Hence the Safe Harbour failed because it was deemed not to ensure adequate level of data protection, *inter alia* because of the lack of effective redress mechanism for individual EU citizens, and also because the Commission had exceeded its powers. With this decision the CJEU also established a criteria for assessing Adequacy Decisions. Hence the *Schrems* case offers a template for the assessment of Adequacy Decisions, such as the Privacy Shield.

As discussed above, the CJEU noted in its judgement that dispute resolution before the FTC was limited to commercial disputes and individual data subjects had no means of recourse against measures of the state.[142] Also the Safe Harbour Decisions did not guarantee any judicial or administrative means to access, rectify or erase data.[143] The Court then proceeded to discuss the requirements of EU law relating to safeguards required for individuals to have the personal data sufficiently protected. The Court considered that interference with fundamental rights

[139] Case C-362/14, *Schrems* case, paras. 98 and 104–105.
[140] Bräutigam, (2016), p. 154.
[141] Bräutigam, (2016), p. 156.
[142] Case C-362/14, *Schrems* case, para. 89.
[143] Case C-362/14, *Schrems* case, para. 90.

guaranteed by Article 7 and 8 of the Charter must be safeguarded.[144] The lack of safeguards was against Article 47 of the Charter guaranteeing the right to effective remedy.[145]

Also the Court stated that the third country in question must ensure 'by way of its domestic law or its international commitments, a level of protection of fundamental rights essentially equivalent to that guaranteed in the EU legal order'.[146] Hence an Adequacy Decision must, according to the decision of the CJEU in the case of *Schrems*, fulfil the requirement of Article 47 of the Charter of Fundamental Rights and to effectively safeguard fundamental right of data protection (Article 8 of the Charter), because legislation that does not allow individuals to pursue remedies does not comply with Article 47.

This set of criteria will be applied to the Privacy Shield in Chapter 4. More specifically I shall be assessing whether the Privacy Shield redress mechanisms offer 1) an independent and impartial tribunal previously established by law, 2) proceedings within reasonable time, 3) fair and public hearing, 4) effective remedy, and 5) the possibility of being advised, defended and represented and legal aid when applicable.

However, it is also necessary here to look into the case law of the CJEU to some extent to determine how the court defines an 'effective remedy' of Article 47 of the Charter[147] and also protection of personal data Article 8, because it is likely that the Court would follow its previous case law to determine the adequacy of the Privacy Shield. I will assess the Privacy Shield I the light of Article 47 in Chapter 4. In Chapter 5 I shall then discuss the potential of balancing data protection with other interest, in particular economic interest.

The Schrems reaffirms the right of data protection.[148] In the event that the validity of the Privacy Shield should come before the CJEU, it is likely that the court would take into consideration its previous case law relating to data protection. And the court has been very protective personal data giving much emphasis on the Charter Articles 8 (and 7).[149] For instance the CJEU has held, in case called Digital Rights Ireland, that in order to ensure effective protection as provided in Article 8 (3) of the Charter which related to control by an independent authority the Data Retention Directive which did not require data to be retained with the EU was not in incompliance

[144] Case C-362/14, *Schrems* case, para. 91.
[145] Case C-362/14, *Schrems* case, para. 95.
[146] Case C-362/14, *Schrems* case, para. 96.
[147] Art. 47, Charter of Fundamental Rights.
[148] Kuner, (2016), p. 9.
[149] Arts. 7 and 8, Charter of Fundamental Rights.

with that Article.[150] The test established in this case for the balancing between data protection and national security was that the access of authorities to personal data had to genuinely satisfy an objective genuine interest, data retention had to be limited to what was strictly necessary.[151]

Another CJEU case that might give some indication about the state of data protection in the EU is Google Spain, where the so called 'right to be forgotten' was founded.[152] In the case the Court found that a search engine was obliged to remove personal data so that the data could not be found using the search engine. The notable thing about the case is, however, that the CJEU very specifically put data protection in front of the economic interests of the search engine.[153] Some commentators think that this establishes a hierarchy of interests, putting data protection before some other interests, such as freedom of expression or the economic interests of a search engine operator.[154]

Although the CJEU has also stated in its other judgements that data protection has to be balanced against other interests, and it is not an absolute right, e.g. in cases of Schecke,[155] Deutsche Telekom,[156] and Schwartz.[157] The CJEU's reasoning does not always seem consistent. On one hand, the Court does recognise that the protection of personal data has to be balanced with other interests, while in some case the Court seems to give significant weight on data protection, as in the *Schrems* case and also in the Digital Rights Ireland case. The Court did not discuss the economic significance of data in its case law, other than making a vague note that national supervisory authorities must be able to make this balancing exercise.[158]

These cases show that the CJEU is willing to give much weight and importance to data protection, even when it is compared to other interests. The Court has a quite a protectionist approach to data protection. It is likely that the Court would take the same approach, if it were to assess the Privacy Shield. The approach of the Court does not as such affect my assessment of the Privacy Shield redress mechanisms. Despite I am using the criteria developed by the Court, I

[150] Case C-293/12 - Digital Rights Ireland and Seitlinger and Others, para. 68.
[151] Case C-293/12 - Digital Rights Ireland and Seitlinger and Others, para. 41 and 52.
[152] Case C-131/12 - Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, para. 98.
[153] Case C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, para. 91.
[154] Brkan, (2016), p. 825. See also Frantziou, (2014), p. 766.
[155] Case C-92/09 and C-93/09, Volker und Markus Schecke and Hartmut Eifert, para. 48.
[156] Case C-543/09, Deutsche Telekom AG v Bundesrepublik Deutschland, para. 51
[157] Case C‑291/12, Michael Schwarz v Stadt Bochum, para. 33.
[158] Case C‑362/14, *Schrems* case, para. 42.

am acting on my own behalf. The Court could disagree and decide differently, if it were to make such a decision. Still it is good to mind the ‘high’ level of protection for personal data.

3. The Privacy Shield and Comparison to the Safe Harbour

3.1. Key Points of the Privacy Shield Arrangement

The European Commission adopted the Privacy Shield Decision[159] on 12 of July 2016. Amongst other things the new framework promises better safeguards against US government access and easier redress for individual EU citizens. The United States gave assurances that access will be limited.[160] The Commission and the United Sates had already agreed upon that it was necessary to replace the Safe Harbour with a new arrangement in February 2016.[161] Discussion about strengthening the Safe Harbour had in fact already started in 2014, but the *Schrems* decision in October 2015 had accelerated the discussion significantly.[162] Also the Article 29 Working Party had given its opinion that putting together a new framework was essential and given the Commission time until January of 2016 to complete a new regime.[163] According to the Commission, the Privacy Shield reflects the requirements set by the CJEU in the *Schrems* ruling.[164]

Most notably the United States Office of the Director of National Intelligence (White House) made a strong commitment ruling out mass surveillance, and also US Secretary John Kerry committed to establishing an independent Ombudsman to provide a redress mechanism in the area of national security. Also the protection of personal data of EU citizens is strengthened by introducing several new and also affordable dispute resolution mechanisms.[165]

The Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (hereinafter referred to as the 'Privacy Shield Decision') is similar to the Safe Harbour Decision in the sense that it also provides a system of self-

[159] 'The Privacy Shield Decision' Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield
[160] European Commission, Press release, IP/16/2461, (2016).
[161] European Commission, Press release, IP/16/216, (2016).
[162] 'The Privacy Shield Decision', Preamble part 1., para. 12.
[163] WP29, *Schrems* Statement, (2015).
[164] European Commission, Press release, IP/16/2461, 12 July 2016.
[165] European Commission, MEMO/16/2462, (2016), p. 2.

certification.[166] It is thus does not determine that United States provides adequate data protection as required by EU law, but similarly to the Safe Harbour, protection is deemed adequate if a US organisation is certified with the regime.[167]

Similarly to the Safe Harbour, transfers of personal data from the EU to the US are only permitted if the US company in question adheres to the Privacy Shield principles.[168] Those are 1) Notice, 2) Choice, 3) Accountability for Onward Transfer, 4) Security, 5) Data Integrity and Purpose Limitation, 6) Access, 7) Recourse, Enforcement and Liability.[169] Like with the Safe Harbour Decision here, it suffices to discuss the principles which relate to redress mechanisms. Thus according to the Recourse, Enforcement and Liability Principle, there has to be 'robust' mechanisms to ensure compliance, which in minimum must include:

> i. readily available independent recourse mechanisms by which each individual's complaints and disputes are investigated and expeditiously resolved at no cost to the individual and by reference to the Principles, and damages awarded where the applicable law or private-sector initiatives so provide;
> ii. follow-up procedures for verifying that the attestations and assertions organizations make about their privacy practices are true and that privacy practices have been implemented as presented and, in particular, with regard to cases of non-compliance; and
> iii. obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations.[170]

The Principle is similar to the Safe Harbour one, but it has been clearly stated that investigation of complaints must be expeditious and free. Also a follow-up procedure must pay particular attention to non-compliance.

In addition to the seven Principles there is also a list of Supplemental Principles, which give more detailed rules how to comply with the Principles.[171] They thus replace the FAQ system of

[166] 'The Privacy Shield Decision', Preamble part 2, para. 14.
[167] 'The Privacy Shield Decision', Preamble part. 2.1., paras. 20–29.
[168] 'The Privacy Shield Decision', Preamble part 2., para. 14.
[169] 'The Privacy Shield Decision', Annex 2, ANNEX II, II. Principles. See also Preamble part. 2.1., paras. 20–29.
[170] 'The Privacy Shield Decision', Annex 2, ANNEX II, II. Principles, 7.a.
[171] 'The Privacy Shield Decision', Annex 2, ANNEX II, III. Supplemental Principles.

the Safe Harbour. Similar to the Safe Harbour, to comply with verification requirements (follow-up procedures), companies can do that through self-assessment or outside compliance reviews.[172] To meet the first and third requirements, recourse mechanisms and remedies, there are choices. Those are same as with the Safe Harbour:

> (i) compliance with private sector developed privacy programs that incorporate the Privacy Shield Principles into their rules and that include effective enforcement mechanisms of the type described in the Recourse, Enforcement and Liability Principle;
> (ii) compliance with legal or regulatory supervisory authorities that provide for handling of individual complaints and dispute resolution; or
> (iii) commitment to cooperate with data protection authorities located in the European Union or their authorized representatives.[173]

Again the list is not meant to be exhaustive, and other alternatives can be used by US organisations as long as they comply with the Principles. Different to the Safe Harbour, the Privacy Shield then lists specifically the recourse options available to individual data subjects. Those are going to be discussed in more detail in the following part.

3.2. Comparison of Safe Harbour and Privacy Shield Redress Mechanisms

In terms of redress mechanisms there have been changes in the Privacy Shield in comparison to the Safe Harbour. The Privacy Shield Decision has a list of redress mechanisms available for individual EU citizens to lodge complaints in case of non-compliance by the US bodies responsible for their personal data. The decision also states that organisations must have independent and readily available recourse mechanism so that disputes can be resolved quickly and with no cost to the individual.[174] Similarly to the Safe Harbour, an organisation may choose which independent recourse mechanisms it wishes to use either in the US or in the EU. Thus they are able to voluntarily cooperate with European national Data Protection Authorities.[175]

[172] 'The Privacy Shield Decision', Annex 2, ANNEX II, III. Supplemental Principles, 7.b.
[173] 'The Privacy Shield Decision', Annex 2, ANNEX II, III. Supplemental Principles, 11.a.
[174] 'The Privacy Shield Decision', Preamble part. 2.3., paras. 38–39.
[175] 'The Privacy Shield Decision', Preamble part. 2.3., para. 40.

EU citizens can choose which route they want to pursue when lodging a complaint. Those are divided to redress mechanisms that are available against actions by independent companies and redress options that are available in case of violations by US public authorities. Redress mechanism against private companies are presented first.

3.2.1. How to Complain about a Private Company

The first avenue available is to lodge a complaint with the company itself. The company must offer a redress mechanism either inside or outside the company and inform individual data subjects about how the complaint can be made. Organisations must provide information on their website about the Privacy Shield Principles and recourse options available with specific instructions on how to make a complaint. The complaint must be investigated and response whether the claim had any merits and whether it will be remedied must be given within 45 days.[176]

The second option is to contact the alternative dispute resolution body if the company in question has chosen as its independent recourse mechanism. This body may be located in the US or the EU. Details of this option must also be given on the website of the organisation. This body must investigate the claim and when appropriate provide effective remedies, which may mean reversing or correcting the effects of non-compliance and even termination of further data processing. Investigation can only be denied on the basis that the claim is obviously unfounded or frivolous. If the company does not comply with the ruling of the alternative dispute resolution body, the US authorities, FTC and the Department of Commerce are notified. Failure to comply with these authorities will result in removal from the Privacy Shield list.[177]

The third option is, if the US company has chosen to cooperate with an EU Data Protection Authority (DPA), the EU data subject can complain directly to the DPA. Thus this is an alternative to the previous option, depending which method the US organisation has chosen. Or in the case of human resources data in the context of an employment relationship, US companies are always required to comply with EU DPAs. Thus an EU citizen can always deal with the

[176] 'The Privacy Shield Decision', Annex 2, ANNEX II, III. Supplemental Principles, 11.d.i.–ii. See also Preamble part. 2.3., paras. 43–44.
[177] 'The Privacy Shield Decision', Annex 2, ANNEX II, III. Supplemental Principles, 11.d.i.–ii. See also Preamble part. 2.3., paras. 45–47.

local DPA, when the employment data is in question. At the DPA the claim is investigated by an informal panel. Both sides have an opportunity to make comments or provide evidence and the panel will give its advice (usually within 60 days of receiving the complaint). The US company must then comply with the advice within 25 days. If it fails to do so without a valid excuse, the DPA can either forward the matter to the Federal Trade Commission (FTC), which can start an enforcement action. Or, alternatively, the DPA can conclude that the breach has been serious and forward the matter to the Department of Commerce (DoC), which has to consider removing the company from the Privacy Shield list. Also the DPA, even though it has not been chosen as the independent recourse option by the company, can still receive complaints by EU data subject and then forward them to the FTC or the DoC. In the case that the local DPA fails to act the data subject can bring an action in a national court of the Member State.[178]

The fourth option is to complain to the US Department of Commerce, but only through a DPA.[179] Thus it may not be as much of another option for EU data subjects to make claims, as the referral to the Department of Commerce is already included in the previous option of complaining to the DPA. Nevertheless the Privacy Shield Decision states in clear terms that the Department of Commerce will establish a dedicated point of contact and issue an update to the complaint within 90 days. It will also contact the violating company to facilitate resolution and if the company does not cooperate it can be removed from the list.[180]

The fifth option is that the EU data subject can complain to the FTC directly. Complaints can also be referred to it by DPAs, independent dispute resolution bodies, EU Member States, or the Department of Commerce. The FTC will give priority to such referrals.[181] Nevertheless, EU citizens can use the same complaint procedure that is offered to US citizens.[182] The FTC provides a system for making complaints online.[183] Compliance is ensured by administering consent orders. The FTC can refer the matter to a court if the company fails to comply. The court

[178] 'The Privacy Shield Decision', Preamble part. 2.3., paras. 48–51. Also if the DPA suspects that and EU company is violating EU data protection law, it can order suspension of the data transfer. See European Commission, Guide to the EU–U.S. Privacy Shield, (2016), p. 16.
[179] 'The Privacy Shield Decision', Preamble part. 2.3., paras. 52.
[180] 'The Privacy Shield Decision', Annex 2, ANNEX II, III. Supplemental Principles, 11.g. See also Preamble part. 2.3., paras.52–53.
[181] 'The Privacy Shield Decision', Annex 2, ANNEX II, III. Supplemental Principles, 11.f. See also Preamble part. 2.3., para. 54.
[182] 'The Privacy Shield Decision', Preamble part. 2.3., para. 54.
[183] FTC complaints on FTC website.

can order civil penalties and remedies. Alternatively, the court can impose an injunction if the FTC seeks it.[184]

The sixth option, the last resort, is that the EU data subject may invoke arbitration at the Privacy Shield Panel. The arbitration will be governed by standard arbitration rules, which will be determined by the Commission and the Department of Commerce. The arbitrators are be chosen by the parties from a pool of arbitrators nominated by the Commission and the DoC. The DPA will assist the EU citizen in the preparations but not the proceedings. And the proceeding may take place via teleconferencing, as the arbitration physically takes place in the United States. However, the data subject will need to pay for his or her attorney's fees. The arbitration panel can impose 'non-monetary equitable relief' to remedy the non-compliance. This is because this redress option is supplementary, and the panel takes into consideration the remedies already awarded through other exhausted avenues of redress. Despite the panel cannot award monetary relief, EU citizens are free to seek such damages through US court system. In that situation remedies can be sought pursuant to the Federal Trade Commission Act. The European data subject has the arbitration option available in all circumstances, except when the company or organisation in question has committed to complying with the EU DPA, or when it is a question of human resources data.[185]

The 'non-monetary equitable relief' could be, for instance, correction, deletion or returning of the personal data to the data subject. Costs, fees, damages or any monetary remedies are not available. Enforcement can be sought after the Federal Arbitration Act in US courts.[186] The remedies offered by any of these above mentioned dispute resolution bodies ought to have the effect reversing or correcting the result of non-compliance. Apart from the Privacy Shield Panel whose powers are limited to granting 'non-monetary equitable relief' bodies can impose sanctions which have to be rigorous to ensure compliance.[187]

Still on top of these options, there are opportunities to seek remedies in US courts. Those action would be governed by US law that may offer remedies under torts law or breach of contract for

[184] 'The Privacy Shield Decision', Annex 2, ANNEX II, III. Supplemental Principles, 11.f. See also Preamble part. 2.3., para. 55.
[185] 'The Privacy Shield Decision', Preamble part. 2.3., paras.56–58.
[186] 'The Privacy Shield Decision', Annex 2, ANNEX I
[187] 'The Privacy Shield Decision', Annex 2, ANNEX II, III. Supplemental Principles, 11.e.

instance.[188] For research economic reasons an in–depth analysis of US law and possible remedies in case of data breaches are left outside the scope of this research. It suffices here to mention that the Obama administration did pass a new law, Judicial Redress Act 2015, under which EU citizens would have similar opportunities to sue US organisations as US citizens under US privacy laws.[189] Instead the focus is solely on the Privacy Shield. Although it must be borne in mind that EU citizens might have other avenues available to them to seek recourse against non-compliance, those options are not assessed in this thesis.

3.2.2. How to Complain about a Public Authority

The novelty of the Privacy Shield Decision is the Ombudsperson mechanism established by the then Secretary of State, John F. Kerry.[190] Such an opportunity was lacking in the Safe Harbour arrangement. Under US law, EU citizens have opportunities to seek remedies against collection and processing of personal data by intelligence agencies.[191] However these do not cover all possible situations and thus the Ombudsperson was established to make sure that all individual complaints are investigated, US law complied with and remedies awarded when needed.[192] This option is thus not the only avenue in seeking redress against US public authorities, rather it is meant to be a 'gap filling' to overcome the limitations that exist in US law preventing EU citizens in bringing claims.

Despite it is established by the US government, the Ombudsperson is independent from US intelligence agencies.[193] He or she will report directly to the Secretary of State who must ensure that the Ombudsperson is not influenced by improper bodies.[194]

---

[188] 'The Privacy Shield Decision', Preamble part. 2.3., para. 59.
[189] See Judicial Redress Act 2015. The WP29 is doubtful whether this is effective since there redress under this act is limited to certain situations only. See WP29 Opinion 01/2016, p. 55–56.
[190] 'The Privacy Shield Decision', Annex 2, ANNEX III.
[191] More specifically there are remedies available in three areas: interference under the Foreign Intelligence Surveillance Act (FISA), access by government officials, and access under the Freedom of Information Act (FOIA). See 'The Privacy Shield Decision', Preamble part. 3.1.2. paras., 111–114.
[192] 'The Privacy Shield Decision', Preamble part. 3.1.2. paras., 115–117.
[193] European Commission, Guide to the EU–U.S. Privacy Shield, (2016), p. 19.
[194] 'The Privacy Shield Decision', Annex 2, ANNEX III, Annex A.1.

Complaints to the Ombudsperson can be made with the assistance of relevant supervisory authorities in the data subjects' own Member States (or the local DPA).[195] The Ombudsperson will investigate the claim and also request for information if needed and then give a response whether US law has been complied with and if not, the intelligence agency in question has to provide remedies. The Ombudsperson will not give information whether the individual in question has actually been a target of surveillance. Access to data held by US authorities can be made under Freedom of Information Act (FOIA). Access to records is limited in many ways.[196] Further actions for violations of law can be made to relevant Government Bodies.[197] The European Commission is satisfied that this mechanism effectively satisfies the requirements set in the *Schrems* case.[198]

The following chart summarises what changes the Privacy Shield has brought in comparison to the Safe Harbour:

[195] European Commission, Guide to the EU–U.S. Privacy Shield, (2016), p. 20.See also, 'The Privacy Shield Decision', Annex 2, ANNEX III, Annex A.1. See also Preamble part. 3.1.2. para., 119.
[196] 'The Privacy Shield Decision', Annex 2, ANNEX III, Annex A.4. and 5. See also Preamble part. 3.1.2. paras., 119–121.
[197] 'The Privacy Shield Decision', Annex 2, ANNEX III, Annex A.6.
[198] 'The Privacy Shield Decision', Preamble part. 3.1.2. paras. 122–124.

	Safe Harbour	**Privacy Shield**
Redress against Private Organisations		
Company	Yes.	Yes.
Self-regulatory supervisory authority or dispute resolution body (EU or US)	Yes, if the US organisation had chosen this method.	Yes, if the US organisation has chosen this method.
European Data Protection Authority (DPA)	Yes, if the US organisation had chosen this method.	Yes, if the US organisation has chosen this method. Always, when employment data is in question.
Department of Commerce (DoC)	Disputes could be forwarded from the DPA or the self-regulatory supervisory body.	Only through a DPA. (Through a dispute resolution body if the US company fails to comply with the judgement of that body.)
Federal Trade Commission (FTC)	Yes, if the US organisation had chosen this method. Disputes could be forwarded from the DPA or the self-regulatory supervisory body.	Yes. Disputes can also be forwarded from the DPA, dispute resolution body, DoC or EU Member States.
Privacy Shield Panel	N/A	Yes, as last resort.
US Courts	Unclear whether possible.	Yes. But subject to limitations of US law.
Redress against Public Organisations		
Ombudsperson	N/A	Yes.
US Courts	N/A	Subject to limitations of US law.

4. Assessment of the Privacy Shield

4.1. Assessment of the Privacy Shield in Light of the *Schrems* Criteria

Now that I have explained how the Privacy Shield works and in particular what redress mechanism are available under this regime, I will assess it using the criteria established by the CJEU in the case of *Schrems*. The set of criteria is, as was discussed above in Chapter 2, that an Adequacy Decision must fulfil the requirement set in Article 47 of the Charter[199] to effectively safeguard the fundamental right of data protection (Article 8[200]) as well as individual privacy (Article 7)[201]. Individuals must be able to seek effective remedies through a tribunal that is independent, impartial and previously established by law.[202]

The CJEU held in the *Schrems* that 'the third country concerned in fact ensures, by reason of its domestic law or its international commitments, a level of protection of fundamental rights essentially equivalent to that guaranteed in the EU legal order.'[203] Hence the Court has decided that the United States does not offer effective data protection, i.e. it is incompatible with the Charter.[204] It also means that the level of protection guaranteed by the Charter must be essentially equivalent, even when data is transferred to the US.

However, Article 47 has a very close connection with Article 6 of the European Convention on Human Rights (ECHR)[205]. Thus I will also use the case law of the European Court of Human Rights (hereinafter referred to as ECtHR). I shall assess all the redress mechanisms offered by the Privacy Shield in the light of this set of criteria one by one. Because the redress mechanisms are different for claims against private actors and public ones, I will discuss them separately, starting with the redress mechanisms that are offered against actions by private organisations. Then I will also assess the regime as a whole, in order to determine whether the Privacy Shield redress mechanism system is too complicated.

[199] Art. 47, Charter of Fundamental Rights.
[200] Art. 8, Charter of Fundamental Rights.
[201] Art. 7, Charter of Fundamental Rights.
[202] Ustaran, Pt. 2, (2016), p. 4.
[203] C-362/14, *Schrems* case, paras. 73, 96.
[204] NiLoidean, (2016), p. 4.
[205] Art. 6, European Convention on Human Rights.

4.1.1. Redress Mechanisms Against Private Companies

Firstly, an option is to complain to the company itself. This option obviously does not fulfil the requirement of 'an independent and impartial tribunal previously established by law' as required by Article 47(2) of the Charter. However, for effectiveness' sake, it is good that data subjects have the option of dealing with the company itself in the first place. The dispute could potentially be dissolved without even referring to an outside tribunal, and time and resources could thus be saved. The timeframe of 45 days that is given to organizations to respond to complaints seems reasonable[206] enough, if it leads to a satisfying result for the data subject. The effectiveness of this route is also dependent on how well do organizations provide information about the availability and the process of making complaints. It is also notable (with all of the redress options) that data subject must have access to their data, to have knowledge about a potential breach in the first place.

Secondly, one can refer the complaint to the independent dispute resolution body that the company has chosen. According to CJEU case law, the tribunal that is required in Article 47(2)[207] does not have to be a so called traditional court. The case law of the ECtHR also says the same.[208] The CJEU has stated that the tribunal must be established by law, permanent, have compulsory jurisdiction, have *inter partes* procedure, applies rules of law and is independent.[209] In that case an independent Alternative Dispute Resolution (ADR) body could suffice to satisfy the requirement of Article 47(2), provided that it satisfies the aforementioned requirements.

The tribunal must be independent and impartial. According to the case law of the CJEU, to be independent the tribunal must be acting as a third party, hence not linked to any of the parties in dispute.[210] Impartiality rather relates to the neutrality of the individual decision makers and CJEU has stated that the members of the tribunal must be impartial.[211] Potentially it could be questioned how independent the ADR body chosen by the company itself could be, because the

[206] The CJEU has not established any exact timeframe for proceedings but generally they have to be reasonable. See Case C‑58/12 P, Groupe Gascogne SA v European Commission, paras. 82–88.
[207] Art. 47(2), Charter of Fundamental Rights.
[208] ECtHR, Klass and others v Germany, No. 5029/71, 6 September 1978, paras. 56 and 67.
[209] Case C-54/96, Dorsch Consult Ingenieurgesellschaft mbH v. Bundesbaugesellschaft Berlin mbH, para. 23.
[210] Case C-24/92, Pierre Corbiau v Administration des contributions, para 15. See also Case C-506/04, Graham J. Wilson v Ordre des avocats du barreau de Luxembourg, para 49.
[211] Case C-506/04, Graham J. Wilson v Ordre des avocats du barreau de Luxembourg, para 53.

usual practice in the industry of commercial arbitration is that, the both parties to the dispute choose their arbitrators.[212] Same rule applies to mediation.[213]

The Privacy Shield Decision does not specify any time frame for the dispute resolution body chosen by the company to complete the dispute resolution procedures, so I cannot say whether it would be reasonable as required in the case law of the CJEU.[214] The fact that there is not any timeframe raises a question whether it was intended by the drafters of the Privacy Shield Decision. In any case the lack of timeframe is regrettable and can be seen as a weakness.

Article 47(2) of the Charter also requires fair and public hearing.[215] Fair and public hearing means in the context of EU law that there has to be equality of arms, adversarial proceedings, reasoned decision and judicial execution.[216] The first, equality of arms, relates to the parties' equal opportunity to present their case. According to the CJEU both parties must be given a reasonable opportunity to present their case.[217] Adversarial proceedings on the other hand mean that the parties must be able to examine all documents and comment on them.[218] Reasoned opinion means that the defendant must be able to understand why the decision was made against him or her so that an appeal can be made.[219] The latter, judicial execution means that there has to be an opportunity to seek enforcement in courts. In the context of EU law, public hearing means the right to an oral hearing in person, although that right is not absolute.[220] Hence an independent body can be considered satisfactory from the EU law perspective as long as it satisfies these requirements. So to conclude whether the requirement of fair and public hearing is satisfied, I must say yes, as long as it is consistent with the requirements mentioned above. The Privacy Shield Decision does not specify what the rules of this option are, so it depends.

Article 47(1)[221] also entails that there has to be an effective remedy. According to the Privacy Shield Decisions Enforcement, Recourse and Liability Principle US organisations must remedy problems that arise as a result from the failure to comply with the Privacy Shield.[222] According

[212] Born, (2014), p. 1637.
[213] Hopt and Steffek, (2013), p. 56.
[214] Case C‑58/12 P, Groupe Gascogne SA v European Commission, paras. 82–88.
[215] Art. 47(2), Charter of Fundamental Rights.
[216] Handbook on European law relating to access to justice, (2016), p. 40.
[217] Case C‑199/11, Europese Gemeenschap v Otis NV and Others, para. 71.
[218] Case C‑300/11, ZZ v Secretary of State for the Home Department, para. 55.
[219] Case C‑619/10, Trade Agency Ltd v Seramico Investments Ltd, para 53.
[220] Case C-399/11, Stefano Melloni v Ministerio Fiscal, para. 49.
[221] Art. 47(1), Charter of Fundamental Rights.
[222] 'The Privacy Shield Decision', Annex 2, ANNEX II, II. Principles, 7.a.iii.

to the Privacy Shield Decision this ADR body chosen by the company must be able to afford remedies, such as reversing or correcting the damages suffered or in some situations terminating the data processing altogether.[223] In the case law of the CJEU an effective remedy depends on the circumstances, and the situation must be assessed as a whole.[224] EU law does not require the use of specific remedies, rather, it only sets some standards for remedies and leaves it to the discretion of Member States to decide what exact remedies they want to use. The CJEU has stated that the principle of effectiveness and equivalence must be observed.[225] These relate to the obligation of Member States to ensure the effectiveness of EU law with remedies. Similarly the effectiveness of EU law could be hampered if actors in third countries would not be required to afford effective remedies. In my opinion reversing or correcting the damage seems satisfactory. However, I wonder under what circumstances the processing could be terminated altogether. The Privacy Shield Decision does not specify under which condition it could occur, rather, it only says 'depending on the circumstances'.[226]

Yet one might question the extent and reach of EU law. The CJEU has set some limitations to ensure the effectiveness of EU law, thus limiting the discretion of Member States. Hence actions by the Member States that render the EU law ineffective are not allowed.[227] The question is whether the same rules would apply to an ADR body that is based in the United States. Or, in other words, would that US based ADR body have to comply with CJEU case law and what constitutes and effective remedy. Taking into consideration the *Schrems* case and how the Court considered that the data protection must be 'essentially equivalent'[228] I would conclude by way of analogy, that the US based ADR body would have to comply with the CJEU case laws as regards to what constitutes an effective remedy. The Court noted in its judgement that the level of data protection required could be easily circumvented if the protection in the third country

[223] 'The Privacy Shield Decision', Annex 2, ANNEX II, III. Supplemental Principles, 11.e. See also Preamble part. 2.3., paras. 45–47.
[224] Case C-312/93, Peterbroeck, Van Campenhout & Cie SCS v Belgian State, para. 14.
[225] Case C‑583/11 P, Inuit Tapiriit Kanatami and Others v European Parliament and Council of the European Union, para. 102. 'Equivalence' in the context of EU law means that the national procedural rules that safeguard rights under EU law must not be less favourable than in equivalent domestic situations. 'Effectiveness' on the other hand requires that domestic rules must not render the exercise of EU rights difficult of excessively difficult. See Joined Cases C‑317/08, C‑318/08, C‑319/08 and C‑320/08 Rosalba Alassini v Telecom Italia SpA (C-317/08), Filomena Califano v Wind SpA (C-318/08), Lucia Anna Giorgia Iacono v Telecom Italia SpA (C-319/08) and Multi-service Srl v Telecom Italia SpA (C-320/08), para 48.
[226] 'The Privacy Shield Decision', Preamble part. 2.3., para. 45.
[227] Case C-213/89, The Queen v Secretary of State for Transport, ex parte: Factortame Ltd and others, para. 20. See also: Case C-106/77, Amministrazione delle Finanze dello Stato v Simmenthal SpA, paras. 22–23.
[228]Case C‑362/14, *Schrems* case, para. 73.

was not essentially equivalent. And the purpose of Article 25(6) of the Data Protection Directive is to ensure that the protection accorded in Article 8(1) of the Charter is that the high level of protection continues even when data is transferred to a third country.[229] The same would be true with all the other elements of Article 47 of the Charter. Whether one thinks that the EU is reaching its claws too far outside its jurisdiction is another matter. But for the purposes of protecting EU citizens' fundamental right of data protection it is arguably necessary.

Based on what has been discussed above it can be concluded that as long as the ADR body satisfies the requirements that have been set by the CJEU as regards to Article 47, it can be considered satisfactory. Also according to the Privacy Shield, the matter can be referred to the FTC or the Department of Commerce in the case that the US organisation fails to comply with the decision of the ADR body. I shall discuss these in detail below.

Article 47(2) of the Charter requires also that everyone must have 'the possibility of being advised, defended and represented' and legal aid has to be available where appropriate (Art. 47(3)).[230] The Privacy Shield only requires that the US company in question, as well as the ADR body chosen by the company, must provide information about the complaint procedures.[231] Although anyone could hire a legal assistant to navigate the terms and conditions of making a complaint, there is at least a slight chance of this mechanism not meeting the requirement of article 47, because it depends on how understandable and reader friendly the information is.

Potential problems could arise in filing an eligible complaint, especially if the chosen ADR body happens to be located in the US. For instance, TRUSTe, a US based establishment, which provides dispute resolution in data protection matters, requires a complaint made in English, or the relevant organisation which the data subject wishes to complain about must provide translation.[232] (That can be difficult if the relevant organisation is based in the US.) The geographical location might also be an issue. According to the CJEU the distant location of the court may be an obstacle in bringing proceedings.[233] The CJEU has also stated that mere electronic access is

[229] Case C‑362/14, *Schrems* case, paras. 72–73.
[230] Art. 47(2) and (3), Charter of Fundamental Rights.
[231] 'The Privacy Shield Decision', Annex 2, ANNEX II, III. Supplemental Principles, 11.d.ii. See also Preamble part. 2.3., paras. 43 and 45.
[232] TURSTe website, TRUSTe Privacy Dispute Resolution FAQs. See also the online Dispute Resolution form in TRUSTe Feedback and Resolution System.
[233] Case C‑567/13, Nóra Baczó and János István Vizsnyiczai v Raiffeisen Bank Zrt, para 56.

not satisfactory as it may be impossible or excessively difficult for some people.[234] Although this last argument may have weakened as the digitalisation has progressed. Hence the fact that the ADR body is located in the United States (or even in another EU Member State may be equally difficult to access) might not satisfy Article 47 of the Charter. Fortunately there are national DPAs in EU Member States, potentially able to give legal assistance. DPAs shall be discussed below.

One detail that also caught my attention was that the dispute resolution body can deny the investigation of the claim if it is 'obviously unfounded or frivolous.'[235] The Irish Data Protection Commissioner rejected the claim of Max Schrems on the basis that is was 'frivolous and vexatious.'[236] Whether the choice of wording in the Privacy Shield is an accidental coincidence is hard to tell. However one could wonder what sort of claims could be rejected on the basis that they are 'frivolous'. Potentially even ones that might have the effect of even knocking down the entire Adequacy Decision?

Thirdly, there is an option of starting procedures through the EU Data Protection Authority (DPA). This option is available when the US organisation has chosen to cooperate with the European DPA or when it is a matter of employee data. In other circumstances EU data subjects can still approach the DPA, but then it can only refer the case to the FTC or the Department of Commerce.[237] Hence the national DPA cannot be helpful with the communication either to the US company itself or the chosen ADR body, except in employment data matters and when the company has subjected itself to the oversight of the DPA. The Privacy Shield Decision does not specify whether the DPA can help with mere communication with the US company. Therefore the CJEU might think that dealing with an ADR body located in the US might be 'excessively difficult'.[238]

Nevertheless, in matters that the DPA has powers, I must assess whether it meets the requirements set in Article 47 of the Charter. Under this redress avenue there is an informal panel established by the local DPA that can investigate the claim and then give advice to the US company and if the latter fails to comply with the advice, the matter can be referred to the FTC

[234] Joined Cases C‑317/08, C‑318/08, C‑319/08 and C‑320/08 Rosalba Alassini v Telecom Italia SpA (C-317/08), Filomena Califano v Wind SpA (C-318/08), Lucia Anna Giorgia Iacono v Telecom Italia SpA (C-319/08) and Multiservice Srl v Telecom Italia SpA (C-320/08), para 58.
[235] 'The Privacy Shield Decision', Preamble part. 2.3., para. 45.
[236] Maximillian Schrems v Data Protection Commissioner, [2013 No. 765JR], [2014], IEHC 310, paras. 30–33.
[237] 'The Privacy Shield Decision', Preamble part. 2.3., paras. 48 and 51.
[238] Case C‑567/13, Nóra Baczó and János István Vizsnyiczai v Raiffeisen Bank Zrt, para 56.

or the Department of Commerce.[239] I have already discussed above that according to CJEU case law the tribunal required by Article 47(2) of the Charter does not have to be a court, but it has to be established by law, be permanent, have compulsory jurisdiction, have *inter partes* procedure, applies rules of law and is independent.[240] At first glance an 'informal panel' does not sound to fulfil these requirements, but potentially one ought to rather assess the DPA and whether it fulfils these requirements. The 'informal panel' can be considered a working group within the larger organisation responsible for carrying out the functions of the DPA.

Article 47(2) of the Charter also requires the trial to be completed within reasonable time.[241] In the case law of the CJEU reasonable time is dependent on the circumstances.[242] The time frame of 60 days to give its advice and then allowing 25 days for the US company to comply with it seems reasonable in my opinion. However, one must also note that the data subject might have already waited 45 days to get a response from the company itself.

As already stated above, fair and public hearing means in the context of EU law equality of arms, adversarial proceedings, reasoned decision and judicial execution. Equality of arms seems to be fulfilled as each party must be given opportunity to comment or provide evidence.[243] From the Privacy Shield Decision itself it cannot be said with certainty whether the requirement of adversarial proceedings is fulfilled. It only states that the rules of procedure are established at the particular DPA.[244] Whether the panel gives a reasoned decision is also ambiguous. In the first place it gives advice to the relevant US organisation and only if the latter fails to comply, the panel will conclude that there has been a breach in cooperation and forward the case to the Department of Commerce or refer the matter to the FTC.[245] The Privacy Shield Decision does not indicate whether the panel is obliged to give a reasoned opinion. Perhaps it is also a matter of internal rules of procedure. Lastly the requirement of judicial execution seems to be satisfied at least in the case that the panel fails to act, because the data subject can turn to national courts.[246] However, then there would be an opportunity to remedy the failure of the DPA panel to act rather that the data breach. And when the case is referred to the FTC or the

[239] 'The Privacy Shield Decision', Preamble part. 2.3., paras. 48–51.
[240] Case C-54/96, Dorsch Consult Ingenieurgesellschaft mbH v. Bundesbaugesellschaft Berlin mbH, para. 23.
[241] Art. 47(2), Charter of Fundamental Rights.
[242] Case C‑58/12 P, Groupe Gascogne SA v European Commission, paras. 82–88.
[243] 'The Privacy Shield Decision', Preamble part. 2.3., para. 49.
[244] 'The Privacy Shield Decision', Preamble part. 2.3., para. 49, footnote 44.
[245] 'The Privacy Shield Decision', Preamble part. 2.3., para. 49.
[246] 'The Privacy Shield Decision', Preamble part. 2.3., para. 50.

DoC, the execution becomes dependent on US law and it is questionable whether EU fundamental rights can be enforced there. I shall discuss these two bodies in more detail below.

The question of an effective remedy that is required by Article 47(1) of the Charter is also somewhat questionable under this redress route. The Privacy Shield Decision does not specify whether the DPA panel is actually able to afford any remedies. As discussed above, EU law does not require the use of any specific remedies, but only that the principles of equivalence and effectiveness have to be complied with.[247] It is difficult to say whether the advice given by the panel and the compliance of the US organisation with that advice can constitute an effective remedy. I would suggest that it would as long as it has the effect of correcting or reversing[248] the effects of non-compliance with the Privacy Shield principles. Although, the DPA may in some situations order the suspension of the data transfer.[249] This would have the effects of preventing future damage, but not remedying the effects of non-compliance that have already occurred.

Yet Article 47(2) of the Charter also requires that everyone must have an opportunity to be advised, defended and represented and also Article 47(3) requires legal aid when applicable. The Privacy Shield Decision does not specify whether these options are available. Potentially dealing with a local DPA will be easier in practice than dealing with a US based ADR body for instance. However, the help of the DPA is somewhat limited, as discussed above.

Fourthly, one can complain to the Department of Commerce (DoC). This can only be done through a DPA. I have already discussed above with regards to the DPAs and alternative dispute resolution bodies what the requirements are for in independent and impartial tribunal that is previously established by law as required by Article 47(2) of the Charter.[250] The DoC does not have an *inter partes* procedure, so for that reason it is questionable whether it could satisfy the requirements that the CJEU has set for tribunals.[251] Also the independence of the body could be questioned, because the DoC is part of the US government.[252]

---

[247] Case C‑583/11 P, Inuit Tapiriit Kanatami and Others v European Parliament and Council of the European Union, para. 102.
[248] The Privacy Shield Decision states that remedies must have the effect of reversing or correcting the effect of non-compliance. See 'The Privacy Shield Decision', Annex 2, ANNEX II, III. Supplemental Principles, 11.e.
[249] European Commission, Guide to the EU–U.S. Privacy Shield, (2016), p. 16.
[250] Article 47(2), Charter of Fundamental Rights.
[251] Case C-54/96, Dorsch Consult Ingenieurgesellschaft mbH v. Bundesbaugesellschaft Berlin mbH, para. 23.
[252] Department of Commerce website.

With regards to the reasonable time requirement in Article 47(2) of the Charter the Privacy Shield Decision states that the Department of Commerce will provide an update about the status of the case within 90 days of receiving the referral.[253] As the CJEU has not established any exact time frame I cannot say for certainty whether this is reasonable, but I would argue that it would be somewhat frustrating to have to wait for three months and then receive a response that they are working on it. It must also be remembered that the data subject might have already exhausted other redress options before turning to the DoC.

It is questionable whether the requirement of fair and public hearing that is required in Article 47(2) of the Charter[254] is satisfied. First of all, it is not clear whether there is equality of arms or adversarial proceedings once the case is referred to the DoC. The EU data subject can obviously present his or her case to the local DPA, but the Privacy Shield Decision does not specify whether there should be any contact on part of the DoC to the data subject or whether there is an opportunity to present evidence. Nor is there any mention whether the DoC will give a reasoned decision. Instead, once the DoC has received a complaint from the data subject through the DPA, it can only choose to remove the US organisation from the Privacy Shield list, but it cannot do anything else.[255]

Also with regards to effective remedy that is required by Article 47(1) of the Charter[256], the powers of the DoC are limited to removing organisations from the Privacy Shield list. When the DoC sees that there has been a persistent failure to comply, the US organisation can be removed from the Privacy Shield list.[257] Persistent failure to comply occurs if the US organisation 'refuses to comply with a final determination by any privacy self-regulatory, independent dispute resolution, or government body, or where such a body determines that an organization frequently fails to comply with the Principles to the point where its claim to comply is no longer credible'.[258] There is not any mention of any remedies that the DoC could afford to the data

[253] 'The Privacy Shield Decision', Preamble part. 2.3., para. 52. See also Annex 1 *Facilitate Resolution of Complaints about Non-Compliance*.
[254] Article 47(2), Charter of Fundamental Rights.
[255] 'The Privacy Shield Decision', Annex 2, ANNEX II, III. Supplemental Principles, 11.g. See also Preamble part. 2.3., paras.52–53.
[256] Article 47(1), Charter of Fundamental Rights.
[257] 'The Privacy Shield Decision', Preamble part. 2.3., para. 53.
[258] 'The Privacy Shield Decision', Annex 2, ANNEX II, III. Supplemental Principles, 11.g.ii.–iii.

subject. Only that it will make its best efforts to find a resolution.[259] Although it is not impossible that the resolution or the removal from the list may have the effect of correcting or reversing the effects of con-compliance, I find that the remedies ought to be more clearly stated.

The positive part is that the EU data subject can deal with the local DPA, which will be helpful in terms of logistical and linguistic problems. Potentially the DPA will be able to provide some sort of assistance. Also the DoC will have a specified point of contact and make their best efforts.[260]

Fifthly, it is possible to complain to the Federal Trade Commission (FTC). I have already discussed above what are the requirement of independence and impartially in EU law as well as what are the requirements for a tribunal. This body has the same problem as the DoC, it does not have *inter partes* procedure.[261]

The Privacy Shield Decision does not specify a timeframe for the FTC option, so it cannot be said with certainty if this option would satisfy the requirement of 'reasonable time' as required in Article 47(2) of the Charter. Here it must also be noted that the data subject could have already sought redress through the company, the independent dispute resolution body or the DPA. Thus considerable time could have already passed before even turning to the FTC.

From the Privacy Shield document it cannot be concluded whether the requirements of fair and public hearing of Article 47(2) of the Charter would be satisfied. The resources of the body are seriously limited, privacy issues being only a tiny portion of all the issues it deals with. The Privacy Division of the FTC does not have the means to remedy data breaches or investigate complaints throughout so that both sides can be taken into consideration.[262] At least judicial execution can be sought from US courts on behalf of the FTC.[263]

Article 47(1) of the Charter[264] requires effective remedies. FTC's powers of granting remedies are limited to some extent. First of all, it can only grant remedies when there is actual harm or

[259] 'The Privacy Shield Decision', Annex 1 *Facilitate Resolution of Complaints about Non-Compliance*.
[260] 'The Privacy Shield Decision', Annex 1 *Facilitate Resolution of Complaints about Non-Compliance* and *Increase cooperation with DPAs*.
[261] 'The Privacy Shield Decision', Annex 2, ANNEX II, III. Supplemental Principles, 11.f. See also Preamble part. 2.3., para. 55.
[262] Hoofnagle, (2016), pp. 173–174.
[263] 'The Privacy Shield Decision', Preamble part. 2.3., para. 55.
[264] Article 47(1), Charter of Fundamental Rights.

substantial injury. And any changes to this approach are unlikely because of the political economy of the organisation itself, which prevents a departure from the harm-based approach.[265] Personal data breaches can be complicated and it can sometimes be difficult to show any actual harm. The FTC can order administrative orders, thus requiring the US organisation to cease the data processing. In the case that the organisation fails to comply with this order, the FTC can order civil penalties or refer the case to US courts. The FTC thus cannot provide monetary remedies but they have to be sought through US courts. In addition the FTC can only act if there has been a violation of Section 5 of the FTC Act.[266] I have already discussed the limits of the powers of the FTC with regards to the Safe Harbour. Some notable fields are excluded from its jurisdiction, such as telecommunications, transportation and employment.[267]

From this I would conclude that the remedial powers of the FTC do not seem satisfactory from the European perspective. The mere ceasing of data processing does not have the effect of reversing or correcting the effects of non-compliance and any actual remedies can only be sought through US courts, which adds another hurdle to the process, complicating it even further. Even the sanction that the FTC is able to give to the US company in breach are small.[268]

Sixthly, the 'last resort' of dispute resolution with private companies is the Privacy Shield Panel, an arbitral panel, which EU data subject can refer to if everything else fails. Despite the fact that they could still refer to US courts even after exhausting this avenue.[269] However since this thesis is focused on the redress mechanism offered by the Privacy Shield, I have left a detailed analysis of the US court system outside the scope. This arbitration option is only to be used for residual claims, thus if the violation of the Privacy Shield Principles has not been remedied, or it has been remedied only partially.[270]

As I have stated above, an arbitration panel would be sufficient for a 'tribunal' required by Article 47(2). Also the Department of Commerce and the Commission designate a pool of arbitrator based on their integrity, independence and competence in data protection law. They also have to be independent from any influence of any body.[271] On paper it seems that the

[265] Hoofnagle, (2016), pp. 170–173.
[266] 'The Privacy Shield Decision', Preamble part. 2.3., para. 55. See also Annex 2, ANNEX II, III. Supplemental Principles, 11.f.
[267] WP29 Opinion 4/2000, p. 4. Section 5 of the FTC Act relates to unfair methods of competition. See Federal Trade Commission Act, Incorporating U.S. SAFE WEB Act amendments of 2006, Sec. 5.
[268] Hoofnagle, (2016), p. 172.
[269] 'The Privacy Shield Decision', Preamble part. 2.3., para. 59.
[270] 'The Privacy Shield Decision', Annex 2, Annex I, A.
[271] 'The Privacy Shield Decision', Annex 2, Annex I, F. See also Preamble, part. 2.3., para. 57.

Privacy Shield Decision requires independence and impartiality of the arbitration panel, which is good.

According to the Privacy Shield Decision, the arbitration process has to be completed within 90 days of issuing the proceedings unless the parties agree otherwise.[272] As discussed above the CJEU requires reasonable time which is dependent on the circumstances. In my view 90 days seems a reasonable time for arbitration procedures. However it must also be borne in mind that to get to this stage the EU data subject might have already had to complain to the company itself, then proceed to an independent ADR body or the DPA (whichever applicable), the Department of Commerce and the FTC. A considerable time would likely to have passed before being able to come before the arbitration panel.

With regards fair and public hearing required by Article 47(2) of the Charter[273], the Panel is meant to use well-established arbitration procedures. The Privacy Shield Decision mentions for instance AAA (American Arbitration Association) and JAMS (Judicial Arbitration and Mediation Services).[274] I will not go into detail with the rules these organisations use, but generally the arbitration procedures could satisfy the requirements of equality of arms, adversarial proceedings, reasoned decision and judicial execution.

About the remedies that the Privacy Shield Panel is able to award, the 'non-monetary equitable relief' could be considered satisfactory from the perspective of CJEU case law. As discussed above the remedy ought to be effective but the law does not require the use of specific remedies.[275] Such non-monetary relief as correction, deletion or returning of the personal data to the data subject could be satisfactory. Also since this redress option is only mean to be supplementary, I would conclude that it is satisfactory. However, in a situation where the data subject would have exhausted all the other redress options and not received any monetary relief, it could be disappointing that to receive any monetary damages one would still have to continue to US courts and then be limited by FTCs jurisdiction. Although, since EU legislation does not require the use of any specific remedies, it is unlikely that the lack of monetary relief would be an obstacle to the enjoyment of the rights under Article 47.

[272] 'The Privacy Shield Decision', Annex 2, Annex I, G. 9.
[273] Article 47(2), charter of Fundamental Rights.
[274] 'The Privacy Shield Decision', Annex 2, Annex I, G.
[275] Case C-312/93, Peterbroeck, Van Campenhout & Cie SCS v Belgian State, para. 14.

4.1.2. Redress Mechanisms Against US Public Authorities

The Privacy Shield has an option to seek redress against the actions of US public authorities through the Ombudsperson mechanism. This option was completely lacking under the Safe Harbour regime. I have already mentioned that there may be some opportunities to seek redress under US law, but I have left these outside the scope of this study and instead I shall only focus on this Ombudsperson option, because it was meant to 'fill the gaps' and limitations in US law.[276]

First of all, it is questionable whether an Ombudsperson could be considered an 'independent and impartial tribunal previously established by law' as required by Article 47(2) of the Charter and Article 6(1) of the ECHR.[277] Despite the Privacy Shield assures that the Ombudsperson is independent form the Intelligence Community, it is still a body established under the US government.[278] Researchers at the European Parliament have also raised their concerns for this, that the Ombudsperson is not consistent with Article 47 of the Charter.[279] The WP29 also has the same concern and they also question whether the Ombudsperson is even a tribunal as required by Article 47(2) of the Charter. The tribunal does not have to be a traditional court according to ECtHR case law.[280] The tribunal has to be independent.[281]

The independence of the Ombudsperson has been questioned *inter alia* because he or she would have not full powers to address complaints and could not even tell the data subject whether he or she has been targeted by surveillance activities.[282] WP29 also suspects that the Ombudsperson does not have sufficient investigatory powers.[283] The Privacy Shield Decision only states that Ombudsperson will cooperate with Government bodies and independent oversight bodies, to which I referred to above, and that the Ombudsperson will have all the information necessary to give a response to the EU data subject.[284] It is thus not clear whether the Ombudsperson will have access to all relevant information to conduct a full investigation. In the case law of the CJEU independence means that the tribunal must act as a third party, thus independent from

[276] 'The Privacy Shield Decision', Preamble, paras. 115–116.
[277] Art. 47(2), Charter of Fundamental Rights, and Art. 6(1) of the European Convention on Human Rights.
[278] 'The Privacy Shield Decision', Annex 2, Annex III, Annex A, 1. See also Preamble paras. 116 and 121.
[279] From Safe Harbour to Privacy Shield, (2017), p. 32.
[280] ECtHR, Klass and others v Germany, No. 5029/71, 6 September 1978, paras. 56 and 67.
[281] ECtHR, Kennedy v. the United Kingdom, No. 26839/05, 18 August 2010, para. 167.
[282] From Safe Harbour to Privacy Shield, (2017), p. 32.
[283] WP29 Opinion 01/2016, p. 50.
[284] 'The Privacy Shield Decision', Preamble para. 120.
Art 47(2), Charter of Fundamental Rights.

the parties and also administrative authorities.[285] As regards to impartiality on the other hand, the tribunal must be both subjectively and objectively impartial. The first means that the members of the tribunal must not be biased or prejudiced personally, and the latter, that there sufficient guarantees to exclude legitimate doubts.[286] Assessing the Privacy Shield Decision solely it is impossible to give any definite conclusions about the independence and impartiality, but considering the limited investigatory powers, the independence could be doubted.

Whether the Ombudsperson is a tribunal, is also questionable. I have already discussed above what are the requirements for a tribunal in the case law of the CJEU.[287] From these requirements at least the requirement of *inter partes* procedure does not seem to be fulfilled, because despite the Ombudsperson will communicate with the individual through the responsible complaint handling body (which could be the DPA), the parties are not included in the investigation.[288]

Secondly, considering the time of the proceedings under the Ombudsperson mechanism, the Privacy Shield states, that a response will be given 'in a timely manner'.[289] This vague expression is not very helpful in determining whether this is reasonable as required in EU law.[290] According to ECtHR case law it depends on the circumstances whether it is reasonable.[291] The entire length of the proceeding starting from the initiation to the appellate procedures have to be included in the consideration to determine whether the time is consistent with Article 6.1 of the ECHR.[292] Similarly the case law of the CJEU requires reasonable time.[293] In the absence of information of the exact length of the proceeding within the Ombudsperson mechanism it is impossible to say whether it is reasonable. However, the ECtHR has established that such issues as 'the complexity of the case, the conduct of the applicant and of the relevant authorities and

[285] Case C-24/92, Pierre Corbiau v Administration des contributions, para 15. See also Case C-506/04, Graham J. Wilson v Ordre des avocats du barreau de Luxembourg, para 49.
[286] Joined cases C-341/06 P and C-342/06 P, Chronopost SA and La Poste v Union française de l'express (UFEX) and Others, para. 54.
[287] Namely the tribunal has to be established by law, permanent, have compulsory jurisdiction, have *inter partes* procedure, apply rules of law and be independent. See Case C-54/96, Dorsch Consult Ingenieurgesellschaft mbH v. Bundesbaugesellschaft Berlin mbH, para. 23. According to the case law of the ECtHR tribunal established by law as required by Art. 6(1) of the ECHR, does not have to be a traditional court but has to perform judicial function. See ECtHR, Campbell and Fell v. the United Kingdom, No. 7819/77; 7878/77, 28 June 1984, para. 76.
[288] 'The Privacy Shield Decision', Annex 2, Annex III, Annex A, 4.e.–f.
[289] 'The Privacy Shield Decision', Annex 2, Annex III, Annex A, 4.e.
[290] Art. 47(2), Charter of Fundamental Rights. See also Art. 6(1) European Convention on Human Rights.
[291] ECtHR, König v. Germany, No. 6232/73, 28 June 1978, para. 99.
[292] ECtHR, Poiss v. Austria, No, 9816/82, 23 April 1987, para. 50.
[293] Case C‑58/12 P, Groupe Gascogne SA v European Commission, paras. 82–88.

what was at stake for the applicant in the dispute'[294] must be considered. Potentially the fact that in the context of the Ombudsperson the question could be a matter of national security could mean that the issue is considered complex. It is difficult to confirm this.

Fair and public hearing is also required by Article 47(2) of the Charter.[295] First, it is not clear whether equality of arms is satisfied. The EU complaint handling body will help in making the complaint and if the Ombudsperson needs additional information he or she will contact the EU data subject or the body.[296] Hence, the EU data subject will have some opportunity to present his or her case. However, the Ombudsperson mechanism does not have adversarial proceedings. In the case law of the ECtHR it is required that the parties must have an opportunity to examine and comment the evidence and submissions made by the other party.[297] CJEU case law has the same requirement.[298] Apart from the potential further questions that the Ombudsperson may present to the data subject (or the handling body), the Privacy Shield decision does not require the parties to be able to make comments. The EU data subject will thus not have the opportunity to respond to any claims that the US organisation in question may have put forward. This will make it very difficult to make a claim as it will be impossible to anticipate all the potential arguments that may be made during proceedings.

Reasoned decision is also required.[299] The Privacy Shield decision only states that the Ombudsperson will confirm that the issue has been investigated, US law has been complied with and that when appropriate, remedies have been awarded. The Ombudsperson will not tell if the data subject has been a target of surveillance.[300] It seems that the requirement of reasoned opinion is not satisfied. The lack of sufficient information would make it very difficult to appeal, as is required in the case law of the CJEU[301] and the ECtHR.[302] The CJEU has stated that the reasons

[294] ECtHR, Frydlender v. France, No. 30979/96, 27 June 2000, para. 43.
[295] Art 47(2), Charter of Fundamental Rights. And Art. 6(1), European Convention of Human Rights. I have already stated above that fair and public hearing means be equality of arms, adversarial proceedings, reasoned decision and judicial execution.
[296] 'The Privacy Shield Decision', Annex 2, Annex III, Annex A, 3. and 4.b–c, f.
[297] ECtHR, Ruiz-Mateos v. Spain, No. 12952/87, 23 June 1993, para. 63.
[298] Case C-199/11, Europese Gemeenschap v Otis NV and Others, para. 71.
[299] For ECtHR See ECtHR, Suominen v. Finland, No. 37801/97, 24 July 2003, paras. 36–38. And CJEU, Case C-619/10, Trade Agency Ltd v Seramico In-vestments Ltd, para 53.
[300] 'The Privacy Shield Decision', Annex 2, Annex III, Annex A, 4.e. See also Preamble para. 121.
[301] Case C-619/10, Trade Agency Ltd v Seramico Investments Ltd, para 53.
[302] ECtHR, Hadjianastassiou v. Greece, No. 12945/87, 16 December 1992, para 53. See also Joined Cases C-584/10 P, C-593/10 P and C-595/10 P, European Commission and Others v Yassin Abdullah Kadi, para. 100.

must be 'specific and concrete'.[303] Then finally, there has to be judicial execution. The Privacy Shield Decision does not offer this option, but further actions are referred to the relevant US Government body or independent oversight bodies.[304] Should the EU data subject wish to have access to US Government records under the Freedom of Information Act (FOIA) and denied, appeal can be made first through administrative means and then in federal courts.[305] Judicial execution as such is missing. The WP29 has also understood that the decision of the Ombudsperson is final and judicial execution or appeal is not possible.[306]

Article 47(1) of the Charter[307] also says that there has to be an effective remedy. The same is also required in Article 13 of the ECHR.[308] According to the case law of the CJEU the effectiveness of the remedy depends on the circumstances.[309] The remedy must also be effective and equivalent.[310] The Privacy Shield Decision does not specify what the remedies will be in the case of a public authority violating data protection rules. According to the Supplemental Principles the remedy must have the effect of reversing or correcting the non-compliance. But this seems to only apply to remedies awarded by dispute resolution bodies with dispute with private companies.[311] With the information given in the Privacy Shield Decision it is thus impossible to say whether the remedies awarded to EU data subjects in case of non-compliance by a public authority would be effective as required by EU law. Also, considering that the Ombudsperson shall not confirm whether the EU data subject has in fact been a target or surveillance, makes it impossible to assess whether the remedy is effective.

[303] Joined Cases C-584/10 P, C-593/10 P and C-595/10 P, European Commission and Others v Yassin Abdullah Kadi, para. 116.
[304] 'The Privacy Shield Decision', Annex 2, Annex III, Annex A, 6. See also Preamble para. 120.
[305] 'The Privacy Shield Decision', Annex 2, Annex III, Annex A, 5.d.
[306] WP29 Opinion 01/2016, p. 51.
[307] Art. 47(1), Charter of Fundamental Rights.
[308] Art. 13, European Convention on Human Rights.
[309] Case C-312/93, Peterbroeck, Van Campenhout & Cie SCS v Belgian State, para. 14.
[310] Case C-583/11 P, Inuit Tapiriit Kanatami and Others v European Parliament and Council of the European Union, para. 102. For 'equivalence' and 'effectiveness' see Joined Cases C-317/08, C-318/08, C-319/08 and C-320/08 Rosalba Alassini v Telecom Italia SpA (C-317/08), Filomena Califano v Wind SpA (C-318/08), Lucia Anna Giorgia Iacono v Telecom Italia SpA (C-319/08) and Multi-service Srl v Telecom Italia SpA (C-320/08), para 48.
[311] 'The Privacy Shield Decision', Annex 2, ANNEX II, II. Principles, 11.d.

Article 47(2) does still require the right of being advised, defended or represented and Article 47(3) require legal aid when appropriate.[312] Considering that the 'EU individual complaint handling body' (the DPA) shall be assisting the EU data subject with the submission of the complaint[313] this requirement could be satisfied.

One must note, however, that some other options could be possible for EU citizens to seek redress against the US intelligence agencies. One might do what Max Schrems did and bring an action at the Data Protection Authority, which can suspend the data transfer or refer the case to the national courts. The national court could then further the case to the CJEU, which could then invalidate the Privacy Shield.[314] In my view this option seems tiresome and time consuming. It is also a very long road to seek redress. As mentioned above, an individual could go directly to other US Government bodies. In that instance the relevant Act would be Freedom of Information Act (FOIA), which is limited and likely to result in an unsatisfactory result for the EU data subject. In this case referring to US courts would be the only solution, where an action could be brought under Foreign Intelligence Surveillance Act or some other piece of US legislation.[315]

In my opinion, the Ombudsperson Mechanism is certainly an improvement. After all it does introduce a redress mechanism that was completely lacking in the Safe Harbour Decision. Yet, the new mechanism also raises many questions. The Ombudsperson is meant to investigate whether US law has been complied with, not whether the organisation has complied with the Privacy Shield Principles. This raises the question whether rules are different for public bodies than private ones. And I have already discussed that US data protection law is fundamentally different from EU data protection law, it is sector specific and piecemeal. And the CJEU in the *Schrems* ruling specifically states than an Adequacy Decision would have to satisfy the requirements of Article 8 of the Charter[316] and thus provide effective data protection like guaranteed in that provision. From the Privacy Shield Decision one cannot confidently confirm that such protection is guaranteed. According to the Commission the new arrangement does satisfy the requirements set by the CJEU, because there are a number of new opportunities to seek redress.[317] I would not quite agree.

[312] Art. 47(2), 47(3), Charter of Fundamental Rights. See also Art. 6, European Convention on Human Rights.
[313] 'The Privacy Shield Decision', Annex 2, Annex III, Annex A, 3.
[314] From Safe Harbour to Privacy Shield, (2017), p. 31.
[315] From Safe Harbour to Privacy Shield, (2017), p. 30–31.
[316] Art. 8, Charter of Fundamental Rights.
[317] European Commission, MEMO/16/2462, (2016), pp. 1 and 4.

From these considerations I must conclude that with regards to the Ombudsperson mechanism seems that EU citizens are at the mercy of US law. It is doubtful that EU data subjects can enforce their fundamental right of data protection on the other side of the Atlantic. Nor is this option in line with the requirements set in Article 47 of the Charter.

4.1.3. Overall Assessment of the Privacy Shield Mechanisms

The Privacy Shield has introduced many new innovations in terms of redress mechanism, which can certainly be seen as a positive thing, because many options were lacking under the Safe Harbour. In the field there are mixed opinions about the new redress mechanisms. Some think that the addition of all new redress mechanisms and especially the Ombudsperson would satisfy the requirements set by the CJEU.[318] Others are not as optimistic. The WP29 noted in its opinion to the draft Privacy Shield that the new recourse mechanisms may be too complicated and therefore ineffective. They also raised concerns whether the Ombudsperson is actually effective.[319] Also many privacy activists have though that the system is too complex.[320]

The CJEU in the *Schrems* judgement stated that there has to be an opportunity to seek an effective remedy before a tribunal.[321] This does not necessarily mean that there has to be a judicial remedy before a traditional court. In fact, access to an alternative dispute resolution mechanism can sometimes make access to justice easier and quicker, as the traditional courts are struggling under a heavy caseload. Court proceedings can also be 'heavy' for the individual herself and could even outweigh the benefits of receiving a judicial remedy. It is also not guaranteed that the remedy awarded by a court would be any better than a remedy awarded by some out-of-court arbitral tribunal. Out-of-court dispute resolution can bring multiple advantages, most notable it is generally speedier and more cost effective.[322]

Therefore, in principle, I am not against the fact that the Privacy Shield offers so many redress options that are outside the traditional courts. However, there are quite a few options, especially for proceedings against private companies that the multiple options may seem like a jungle. At

[318] See e.g. Ustaran, Pt. 3, (2016), p. 3. And Deighton, (2016), p. 2. And Khan, Pt. 2, (2016), p. 2.
[319] WP29 Opinion 01/2016, p. 3, 57.
[320] From Safe Harbour to Privacy Shield, (2017), p. 32.
[321] Case C‑362/14, *Schrems* case, para. 95.
[322] Jeretina and Uzelac, (2014), pp. 43–45.

first glance the Privacy Shield seems to offer a multitude of redress options, but a better look into the terms reveals that the system is quite complicated. Not only that that there are gaps and obscurities.

Firstly, if one wishes to bring a claim against a private company, one should approach the US company first. It is not an obligation, and the EU data subject could skip this and go directly to the alternative dispute resolution body chosen by the company, the DPA or the FTC, but it would make sense to try to solve the dispute directly with the company in order to avoid lengthy procedures.

However, if this option is not satisfactory, the data subject may proceed to the alternative dispute resolution body chosen by the company (ADR body), or the DPA if the company has chosen it as its ADR body or in case of human resources data, the DPA option is always available. Or even if the DPA is not the chosen ADR body, or it is not the matter of human resources data, the DPA option is still available, since the DPA can then refer the case to the FTC or the DoC or suspend the data transfer. This can be confusing, but basically the option is between the ADR body or the DPA. Unless the DPA is the chosen ADR body, in which case the only option is the DPA (or one could also skip that and proceed to the FTC directly). From the remedial point of view these two are different. The ADR body ought to be able to afford a remedy that has the effect of reversing or correcting the effects of non-compliance, or terminating the data transfer, whereas the DPA can only refer the case to the FTC or the DoC or suspend the data transfer, but not really afford any remedies. Thus it would seem that the independent ADR may be a better option for the EU data subject despite the fact that there could be practical difficulties in dealing with an ADR body if it is located in the US, like I discussed above. Hence, the remedies could be dependent on which dispute resolution option the US company has chosen.

Then, if the ADR body is not satisfactory or available, the DPA may forward the matter to the DPA or the FTC. Or the data subject may choose to complain to the FTC directly without the involvement of the DPA. If the matter is forwarded to the DoC its powers are limited to removing the relevant US organisation from the Privacy Shield list, but it cannot award remedies for the damage already suffered. FTC's powers of granting remedies are limited as well. First of all, the powers are limited to Section 5 of the FTC Act, which, as I have already stated, excludes some notable fields. And secondly, the FTC cannot award monetary remedies, but those have to be sought through the US courts. Thirdly, the FTC requires substantial damage or actual injury, which in the case of personal data can be hard to prove. Hence, if the independent ADR

body is not available, the remedies available are removal of the US company from the Privacy Shield list and termination of further data transfer. Neither of these would have the effect of remedying the damage already suffered, but rather just preventing further damage. Should the EU data subject still want compensation for the damage suffered he or she has to go to the US courts.

However, there is another hurdle, the Privacy Shield Panel, the last resort. As I have discussed above the powers of the Panel to grant remedies are limited to non-monetary equitable relief. Although monetary remedies are not required either in the case law of the CJEU or the ECtHR, the case may be that there would not be any opportunity to get monetary remedy, if they are not available at the earlier stages either. Although, in my opinion, I do not see that monetary compensation is necessary. A non-monetary remedy, which could be for instance, correction, deletion or returning of the personal data to the data subject, may be satisfactory if it has the effect of correcting or reversing the effect of non-compliance, and thus be in line with Article 47(1) of the Charter.[323]

In data protection issues the remedy concept is complicated. One of the things that is essential for an effective and working redress mechanism system in data protection issues, that the data subjects have access and knowledge about the different redress options available.[324] Also it is difficult to determine what would be the appropriate remedy, especially in cases where there is not material loss.[325] The effectiveness of redress is difficult because 'the characterization of any compensation awarded to individuals is likely to be key in determining its enforceability in third countries.'[326] The main challenges for effective redress in data protection would thus be assessing the 'quantum of damage' and bringing claims against data controllers in third countries.[327]

There is another issue which has become obvious by now. There are a considerable number of steps to be taken, to seek redress and receive an effective remedy. Or there may be, should the first options not be satisfactory. With regards to mandatory dispute resolution before being able to come before a court, the CJEU has considered that such a requirement is not inconsistent

[323] Art. 47(1), Charter of Fundamental Rights. See also 'The Privacy Shield Decision', Annex 2, ANNEX I, B. Available remedies.
[324] Varney, (2016), p. 554.
[325] Varney, (2016), p. 556.
[326] Varney, (2016), p. 560.
[327] Varney, (2016), p. 560.

with the principle of effective judicial protection as long as the settlement is not binding on the parties, it does not cause a substantial delay, the time-barring of claims is suspended and it does not give rise to any costs (or has very low costs).[328]

Out of the six redress options available for challenging private companies, only the last one, the Privacy Shield Panel, bear costs. The other ones are meant to be free of charge. Therefore I might conclude that these options do not give rise to costs that would be inconsistent with the principle of effective judicial protection. The Privacy Shield Decision does not specify whether claims would be time barred, so I cannot asses that. With regards to substantial delay, there is a chance that the very complicated structure of the redress routes of the Privacy Shield may impose an obstacle to the principle of effective judicial protection. For instance, the procedure could have taken 45 days at the company itself, then 60 + 25 days at the DPA, 90 days at the DoC and then another 90 days at the Privacy Shield Panel, thus adding up to 310 days. Of course the procedure may not take this long, but it could. The procedures could thus cause substantial delay. Lastly, the procedure must not prevent the parties from bringing judicial proceedings, i.e. be binding. The Privacy Shield does not prevent this, although there may be obstacles under US law.

For this I would conclude that I agree with the WP29 that the system for the complaints against private companies is very complicated which may result in the ineffectiveness of the entire system. This ineffectiveness may then result that effective redress is not available and thus the requirements of Article 47 of the Charter are not fulfilled, which in turn means that there are not effective safeguards to protect personal data and the Right under Article 8 of the Charter.

Judicial remedies are not always the most effective means, inconsistencies in the application of the law and the availability of remedies, and most importantly when a third country is involved, the problems of jurisdiction, lead to gaps in redress. Although when it comes to third countries, ensuring effective redress is more difficult because the procedural steps, approach of courts and resources that are available to supervisory authorities may significantly differ.[329]

The courts are not always the best places to seek redress and different out-of-court dispute resolution options may actually be more effective means of seeking redress. They can be quicker and more cost-effective ways of solving disputes (and also lightening the caseload of

[328] Joined Cases C‑317/08, C‑318/08, C‑319/08 and C‑320/08 Rosalba Alassini v Telecom Italia SpA (C-317/08), Filomena Califano v Wind SpA (C-318/08), Lucia Anna Giorgia Iacono v Telecom Italia SpA (C-319/08) and Multiservice Srl v Telecom Italia SpA (C-320/08), paras. 54–57, 67.
[329] Varney, (2016), p. 567.

traditional courts). However, if their powers of granting remedies are limited, they do not really offer a good alternative to the courts, nor are they satisfactory from the point of view of EU fundamental rights, most notable Article 47 of the Charter. Additionally such a complicated system, where there are several instances with slightly different powers, creates an environment where the case can always be forwarded to another body and nobody is responsible of ensuring that the damage or injury suffered is properly remedied.

With regards to claims against US public authorities, there are other opportunities to seek redress under US, other than the Ombudsperson mechanism that I have reviewed above.[330] Since I have left review of US law outside the scope of this study, so I shall not say anything about those other options. The Ombudsperson mechanism itself is relatively straightforward, despite fact that the Ombudsperson may not have sufficient investigatory powers and not being able to confirm if the EU data subject has been targeted by surveillance. (Although if a remedy has been awarded, would that not be an indication that there has been a breach of some sort?)

Yet, the claims against US public authorities could be barred at an early stage. When the individual EU data subject wishes to raise a complaint against a US public authority, the DPAs can help to make sure that the submission is complete.[331] This is good, as it will be considerably easier to deal with a local body, even just for linguistic reasons, but the DPAs still seems to have a considerable power to bar certain claims. The Privacy Shield decision says that the claim must not be 'frivolous, vexatious, or made in bad faith.'[332] As I mentioned above the Irish Data Protection Commissioner rejected the claim of Max Schrems on the basis that it was frivolous and vexatious.[333] Although I do think it is pointless of exhausting the Ombudsperson with completely ridiculous and unfounded claims, I must say that the terms 'frivolous' and 'vexatious' are rather vague. The claim of Max Schrems was considered frivolous because the Commission had already decided that the level of data protection in the US was adequate under the Safe Harbour arrangement, but then it turned out that it was not. I question, how to define 'frivolous' or 'vexatious' in the context of data protection?

Hence I have assessed the redress mechanism offered in the Privacy Shield using the criteria established by the CJEU in the *Schrems* case. The question is whether the Privacy Shield would

[330] E.g. under the Foreign Intelligence Surveillance Act (FISA). Access to documents could be sought through the Freedom of Information Act (FOIA). See Commission Implementing Decision (EU) 2016/1250 'The Privacy Shield Decision', Annex 2, Annex VI, V. Redress.
[331] 'The Privacy Shield Decision', Annex 2, Annex III, Annex A, 3. See also Preamble para. 199.
[332] 'The Privacy Shield Decision', Annex 2, Annex III, Annex A, 3.b.iv.
[333] Maximillian Schrems v Data Protection Commissioner, [2013 No. 765JR], [2014], IEHC 310, paras. 30–33.

pass that test. Considering all the thing discussed above, although I think that the Privacy Shield is certainly an improvement in comparison to its predecessor the Safe Harbour, I have to conclude that in my opinion the redress mechanism of the Privacy Shield are not in concordant with the Article 47 of the Charter[334], particularly with regards to the difficulties in seeking redress because of the complicated structure and the necessity of exhausting sometime several different dispute resolution stages and also the time delays that this is going to cause. The test set by the CJEU would thus not be passed.

Max Schrems calls the Privacy Shield a 'soft update' to the Safe Harbour and 'absolutely laughable', because it does not address the issues raised by the CJEU.[335] I agree with him. And I must add that because of the lack of effective redress options, the Privacy Shield does not effectively guarantee the right to protection of personal data as it is found in Article 8 of the Charter of Fundamental Rights, because the requirements of Article 47 of the Charter are not sufficiently met. And it is Article 47 of the Charter that in the last place has the effect of guaranteeing the rights of the Charter. Without it, the right to protection of personal data would be nothing but a dead letter. Despite the Privacy Shield has introduced improvements compared to the Safe Harbour, those only seemingly improve data protection.

A word or two ought to be said about the possibility of limiting the access to justice. In the case law of the CJEU it has been established that the principle of proportionality must be taken into consideration and limitations of rights must not go beyond what is necessary and appropriate.[336] Although fundamental rights must be in certain circumstances reconciled with other interests.[337] The question is whether the economic interests of the data-driven economy an override the right to data protection and access to justice. Fundamental rights can be restricted only to attain objectives of general interest and the restriction cannot be disproportionate.[338] Given the importance and weight that the CJEU has given to data protection in the recent years especially

[334] Art. 47, Charter of Fundamental Rights.
[335] Schrems, (2016), p. 148.
[336] Joined cases C-92/09 and C-93/09, Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v Land Hessen, para. 74. See also Case C-58/08, The Queen, on the application of Vodafone Ltd and Others v Secretary of State for Business, Enterprise and Regulatory Reform, para 51.
[337] Case C-73/07, Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy, para. 53.
[338] Joined Cases C‑317/08, C‑318/08, C‑319/08 and C‑320/08 Rosalba Alassini v Telecom Italia SpA (C-317/08), Filomena Califano v Wind SpA (C-318/08), Lucia Anna Giorgia Iacono v Telecom Italia SpA (C-319/08) and Multiservice Srl v Telecom Italia SpA (C-320/08), para. 63.

with regards to balancing it with national security[339] or economic interest[340] I would anticipate the scale to turn towards data protection.

4.2. Effects of EU Data Protection Reform

As I mentioned in Chapter 1, EU data protection legislation in going through a reform. That is why it is necessary to take that into consideration. The Data Protection Directive (DPD)[341] will be replaced by the General Data Protection Regulation (GDPR)[342] and also by a directive that relates to data protection in the field in crime prevention.[343] The details of this reform are not necessary here. However, the GDPR, which will become fully applicable in May 2018,[344] may have implications on the ability of EU citizens to seek redress from US data processors and controllers, so I must briefly discuss those changes. The regulation shall not have an effect on the validity of the Privacy Shield, which shall remain in force,[345] but certain changes extend the reach of Union law. Also as I mentioned in Chapter 2, the 'adequacy requirement' of EU law for data transfers outside the Union and Adequacy Decision remains in place.[346] Importantly also the Commission when deciding on the adequacy must take into consideration *inter alia* 'effective administrative and judicial redress for the data subjects'.[347]

The GDPR takes a significant step towards regulating transborder data flows.[348] The most notable change is increased territorial scope. Thus the rules of the regulation shall apply to also non-EU based businesses, such as US companies, when they are offering goods and services or monitoring EU behaviour.[349] For the EU data subject that means that he or she can rely on all

[339] See Case C-293/12 - Digital Rights Ireland and Seitlinger and Others, para. 41 and 52.
[340] See Case C-131/12, Google Spain SL, para. 91.
[341] Directive 95/46/EC, (Data Protection Directive).
[342] Regulation (EU) 2016/679, (General Data Protection Regulation).
[343] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.
[344] Reform of EU data protection rules (website).
[345] Art. 96, General Data Protection Regulation. See also 'The Privacy Shield Decision', Preamble part. 2., para. 15
[346] Art. 45, General Data Protection Regulation.
[347] Art. 45(2)(a), General Data Protection Regulation.
[348] Mouzakiti, (2015), p. 51.
[349] Art, 3(2), General Data Protection Regulation. See also Official Website of the GDPR.

the rights guaranteed in the regulation even when the data controller or the processor is based in the US. Reviewing all of them is outside the scope of this study, but I shall discuss the relevant provisions of the regulation that relate to the ability data subjects to seek redress.

Hence, first of all, the data subject will be able to make a complaint with the supervisory authority in their own Member State.[350] Also proceedings can be brought in the courts of the Member State where the data subject is resident.[351] This will make the complaint procedure easier in practice and satisfy the requirement of 'an independent and impartial tribunal previously established by law' of Article 47(2) of the Charter.[352]

The data subject shall also have a right to an effective remedy.[353] There is a right to compensation for any material or non-material damage caused.[354] The GDPR does not make any reference as to what exactly would be the adequate remedy for data protection breaches.[355] But if it satisfies the requirements of effectiveness and equivalence set by the CJEU it ought to be sufficient.[356] The requirement of an 'effective remedy' in Article 47(1) of the Charter[357] would thus be satisfied.

One important difference to note is that the Privacy Shield only applies to processing of personal data by US organisations in the case that the processing does not already fall within the scope of Union legislation.[358] The new GDPR could thus limit the extent of the Privacy Shield.

[350] Art. 77(1), General Data Protection Regulation.
[351] Art. 79(2), General Data Protection Regulation.
[352] Art. 47(2), Charter of Fundamental Rights.
[353] Art. 79(1), General Data Protection Regulation.
[354] Art. 82(1), General Data Protection Regulation.
[355] Varney, (2016), p. 566.
[356] For 'effectiveness' and 'equivalence' see Case C‑583/11 P, Inuit Tapiriit Kanatami and Others v European Parliament and Council of the European Union, para. 102
[357] Art. 47(1), Charter of Fundamental Rights.
[358] 'The Privacy Shield Decision', Preamble part. 2., para. 15

5. Conclusions

5.1. Thoughts on Redress Mechanisms

In the previous Chapters I have assessed the redress mechanisms of the Privacy Shield using the *Schrems* criteria. The CJEU established in that case that individuals must have the right to effective judicial protection and seek remedies, as required by Article 47 of the Charter.[359] By reviewing the redress mechanisms of the Privacy Shield in light of Article 47 of the Charter I came to the conclusion that, in my view, the Privacy Shield would not pass the test. Despite the Privacy Shield is a significant step from the Safe Harbour, it is not quite satisfactory. In this part I wish to summarize what has been discussed throughout this study and add my own thoughts.

The Privacy Shield introduced many improvements compared to the Privacy Shield, more redress mechanisms also against public authorities. The Ombudsperson is arguably the most important addition. I also find that it is good that the European Data Protection authorities (DPAs) have slightly better opportunities to help EU citizens under the Privacy Shield, even if only by assisting with the communication with US organisations or by forwarding the case to US authorities. In that sense it is a step up.

However, there are still deficiencies. The first point I already mentioned in the previous Chapter, the remedies may be dependent on the dispute resolution method chosen by the US company. I came to the conclusion that since the independent ADR body can accord remedies which have the effect of reversing or correcting the effects of non-compliance or even terminating the processing, it would be a better option than the DPA, which does not have powers like these. The latter can only refer the case to the FTC or the DoC. The former can only do so if the US company in question fails to comply with its judgement. This means two things. For one, if the ADR body is the chosen method, there is an opportunity to receive an effective remedy or as required in article 47(1) of the Charter and the case law of the CJEU. For two, if the chosen

[359] Case C-362/14, *Schrems* case, para. 95.

method is cooperation with the DPA, remedies available are dependent on the powers of the FTC and the DoC.

The DoC can only try to find a resolution or remove the company from the Privacy Shield list. It is unclear whether these could be a good and satisfactory remedies. Similarly the powers of the FTC to grant remedies are limited. I already mentioned that certain fields are excluded from the jurisdiction the FTC. Further remedies would still have to be sought through US courts. It is unclear whether either of these options can be satisfactory from the European point of view.

It is questionable whether the FTC and the DoC have powers to reverse or correct the effects of non-compliance. Thus it can be also be concluded that access to an effective remedy may be depended on the dispute resolution body that the US company has chosen. It means that if the chosen body is the DPA, there might not be an opportunity to seek an effective remedy. One can really question why the different redress routes of the Privacy Shield lead to such different results. This can lead to courtroom shopping, the EU data subject has to think what end results he or she wants to achieve.

The second criticism I wish to make is that the Privacy Shield Panel as a last resort is misleading. As access to US courts even after the arbitration of the Panel is still possible, although it could be limited by rules of US law. I also noted that the fact that the Panel cannot award monetary remedies can be disappointing, especially if such remedies have not been awarded at the earlier stages. Despite monetary remedies are not required in the case law of the CJEU, in my view there ought to be an opportunity to seek them, especially if financial losses have been suffered as a result to non-compliance with the Privacy Shield. For instance in the case law of the ECtHR it has been established that 'a remedy must be capable of remedying directly the impugned state of affairs.'[360] I am questioning whether, if the loss suffered is pecuniary, can a non-monetary compensation directly remedy it. One could argue that it would not. Despite monetary remedies could then still be sought in US courts, one could the question whether the process is the too complicated and lengthy.

Which brings me to my next point, which is the requirement of ADR before access to traditional courts. I came to the conclusion that ADR as such is not restricting the enjoyment of the rights under Article 47 of the Charter. In fact, ADR can sometimes offer an easier and more effective redress route, which can be a positive thing for both the EU citizen and the US organisation in

[360] ECtHR, Vučković and Others v. Serbia, No. 17153/11 and 29 other cases, 25 March 2014, para. 74.

question. However, the complexity of the redress mechanism and the multiple steps to be taken could mean that it is not acceptable from the perspective of EU law. I referred to CJEU case, where the court decided that as such ARD is not a problem, as long as does not cause a substantial delay, the time-barring of claims is suspended and it does not give rise to any costs (or has very low costs).[361] I have left the compatibility of ADR and Article 47 of the Charter outside the scope of this thesis, and therefore I am not going to discuss this further. Suffices to note here that, in my view, I do not see why an out-of-court dispute resolution mechanisms could not satisfy the requirements of Article 47, but then that ADR body ought to have sufficient powers to conduct fair procedures and award effective remedies. And as was stated above, not all the bodies that are empowered to solve these disputes under the Privacy Shield seem to have such powers.

Somewhat related to this is the requirement of independent and impartial tribunal, as required by Article 47(2) of the Charter. In fact, the independence of all of the Privacy Shield 'tribunals' could be questioned. In my view the most suspicious is the Ombudsperson, which, as I have discussed, does not seem to have very extensive powers to conduct independent investigations.

I also concluded that the Privacy Shield is quite complex, thus agreeing with the WP29 and many privacy activists.[362] The fact that there can be multiple redress routes to exhaust is certainly evidence that the system is complex. Another issue that adds to the complexity is the issues that I have elaborated above, the choice of the recourse mechanisms by the US company may lead to different results as far as remedies and also the procedures conducted. Related to the complexity is the time of the proceedings. If the EU data subject has to exhaust multiple redress steps, the length of the proceedings could extent to what could be considered unreasonable, thus incompatible with the requirement of reasonable time of Article 47(2) of the Charter. According to CJEU the reasonableness is dependent on the circumstances.[363] I question, whether the complexity of the Privacy Shield redress mechanisms and the multiple steps can be justify lengthy proceedings.

In addition, the procedures vary. I have discussed in the previous Chapter that the requirement of fair and public hearing that is required by Article 47(2) does not seem to be satisfied, at least

[361] Joined Cases C‑317/08, C‑318/08, C‑319/08 and C‑320/08 Rosalba Alassini v Telecom Italia SpA (C-317/08), Filomena Califano v Wind SpA (C-318/08), Lucia Anna Giorgia Iacono v Telecom Italia SpA (C-319/08) and Multiservice Srl v Telecom Italia SpA (C-320/08), paras. 54–57, 67.
[362] See e.g. WP29 Opinion 01/2016, p. 3, 57, and From Safe Harbour to Privacy Shield, (2017), p. 32.
[363] Case C‑58/12 P, Groupe Gascogne SA v European Commission, paras. 82–88.

not with the DPA, FTC, DoC and the Ombudsperson alternatives. Or more precisely, from the Privacy Shield document itself it cannot be said with certainty that the requirement is satisfied.

Further criticism is about the Ombudsperson. I do see it as a massive improvement, that the Privacy Shield introduced a mechanism to seek redress against US public authorities. Still I came to the conclusion that the Ombudsperson is a rather odd procedure where the EU data subject cannot have much say in the proceedings. Nor can the effectiveness of the potential remedies be assessed since the Ombudsperson does not confirm whether the EU data subject has even been a target of surveillance. Although I do understand that this issue falls under the very sensitive top secret category, since it is a matter of US national security, I still think that from the viewpoint of EU data protection law and Article 47 of the Charter, this is not satisfactory.

From these considerations and also the discussions in the previous Chapters I would thus argue that the Privacy Shield would not pass the criteria established by the CJEU in the *Schrems* case. Hence I share my doubts about the Privacy Shield with Max Schrems, who does not believe in the regime.[364] In particular, I think it the remedies are not necessarily effective under all the redress options. Fair and public hearing is not always satisfied, the independence and impartiality of the different options could be questions and lastly, the potentially lengthy procedure might not satisfy the requirement of reasonable time.

Yet, I also discussed the data protection legislation reform in the EU and what changes the GDPR could bring in terms of EU data subject being able to seek redress from US data processors. I think the extended reach of EU data protection law, the increased territorial scope could have its effect. Although, the new regulation may potentially strengthen the rights of EU data subjects, it should not have an effect on the compatibility of the Privacy Shield Decision with EU law and CJEU case law.

5.2. Tension between Data Protection and the Economy

As I have discussed in Chapter 1 and 2, the aim of the EU data protection legislation is not merely the giving effect to the fundamental right of data protection, but also the free flow of

[364] Schrems, (2016), p. 148.

data. That data has extensive economic value, and the free flow of data can lead to major economic advancements. The dual objectives of EU data protection legislation are not the main focus of this study. They are nevertheless important, and therefore I shall only make a brief note about them.

When the *Schrems* decision was made, the invalidation of the Safe Harbour has an immediate effect, putting the data transfers across the Atlantic to a complete halt, until organisations were able to negotiate other means of transferring personal data. Decisions of the CJEU can have a very strong impact restricting international data flows. From an economic perspective this is not desirable. The approach of the CJEU is that the data protection in the third country where the data is transferred has to be 'essentially equivalent.'[365] This sets the standard very high.

Invalidation of the Adequacy Decision has a direct effect on the economy, because the restriction of data flows leads to economic losses. But the CJEU could also indirectly effect data flows and the economy. By setting the standards of data protection high, the Court could have the indirect effect of isolating EU from the world markets, if the third countries, such as the US will not comply with those standards.[366] Some think that the Court does not take into consideration that EU has to function on a global scale.[367] US firms feel increasingly pressured by European data protection rules and even the fear that EU law may become de facto standard. The Europeans are afraid of being subjected to data protection laws that do not reflect their interest. Also American firms reluctant to accept EU Adequacy Decision rules and Europeans are reluctant to US data protection as adequate. When there is a deep disagreement about the basic values of data protection any optimal solution could be deemed as illegitimate on either side of the Atlantic.[368]

The implications of CJEU case law on economy would require further study. Nevertheless, I saw it as appropriate to make a point that the decisions of the Court could have such effects and those ought to be taken into consideration, when determining the faith of the Adequacy Decision. That should also be the responsibility of the Court, since in its own case law it has stated that data protection is not an absolute right and has to be reconciled with other interest.[369]

---

[365] Case C‑362/14, *Schrems* case, para. 73.
[366] Varotto, (2016), p. 10.
[367] Azoulai and van der Sluis, (2016), pp. 1364–1367.
[368] Kobrin, (2014), p. 128.
[369] See e.g. Case C-92/09 and C-93/09, Volker und Markus Schecke and Hartmut Eifert, para. 48, Case C-543/09, Deutsche Telekom AG v Bundesrepublik Deutschland, para. 51, and Case C‑291/12, Michael Schwarz v Stadt Bochum, para. 33.

5.3. Suggestions and Solutions

In this part I wish to review some suggested solutions to address these problems that I have discussed throughout this study and make some suggestions of my own. I have not reviewed all potential suggestions, but only I wish to discuss some that are, in my view, most viable.

A good suggestion in my opinion would be cooperation between the relevant US and EU data protection authorities allowing easier access to redress. This suggestion was put forward at an International Privacy Conference. According to this suggestion information should be made available how to exactly bring a claim in data protection issues. Also the Article 29 Working Party, DPAs and the FTC ought to collaborate in dealing with cross-border complaints.[370] This option would not require any heavy legislative changes and could thus be achieved with relative ease. This is good, because some basic guidance in bringing claims and seeking redress from a data processor located in a third country is arguably needed for EU data subjects. And as this research has shown the redress mechanisms under the Privacy Shield are complicated. However, mere information as to how to bring claims would not solve the other problems with the Privacy Shied, such as questionable independence of the bodies responsible for dispute resolution, the lack of fair and public hearing and effective remedies.

Another solution that have been suggested to solve transatlantic data protection problems is an intergovernmental body that would have the power to pass guidelines and try to find the political consensus.[371] This could ultimately lead to a new bilateral agreement between the EU and the US, or potentially making changes to the existing one. In my view, this option is considerable in the long run, although it would take too much time to solve immediate issues. Also, some think that international law would have little to add because of national security exceptions the limits of international human rights law.[372] Given the fundamental difference in the approach to data protection by the EU and US, co-operation could also be difficult. The history of international co-operation in consumer protection issues in electronic commerce has not been very successful and it would be unrealistic to expect that consensus could be achieved over data protection.[373]

[370] Privacy Bridges, (2015), p. 6 and 29–30.
[371] Varotto, (2016), p. 12.
[372] Irion, (2015), p. 88.
[373] Kuner, (2011), p. 28.

One option would be giving the European data protection authorities more powers in terms helping EU citizens seeking redress from US actors. As discussed above, the powers of the DPAs are limited to some extent. For instance the WP29 has suggested that the DPAs could assist to navigate the US legal system as well as a help with language difficulties.[374] According to the Privacy Shield, the DPAs already have a role of assisting EU data subjects in seeking redress, such as with the Ombudsperson. But potentially, the powers could be extended, so the DPAs could assist in all matters. That would make dealing with the US organisations, and also ADR bodies that are located in the US, easier in practice. Although that would mean that the resources of the DPAs would have to be significantly raised. Rules would also have to be defined, for instance, whether the DPA is meant to give legal assistance. In my view, there could be at least a contact point who could give information, how to start proceedings and what options there are.

It has also been suggested that EU data subject ought to be able to bring claims in EU courts as well as US organisations ought to sue ADR bodies located in the EU, so that EU citizens would have easier access to justice.[375] Being able to access courts on European soil would ease the dispute proceedings significantly. And with the territorial expansion of the GDPR that may soon become a reality. It is not all clear, though, how keen US companies would be about this.

Also the entire Adequacy Decision system could be abolished. According to Kuner, the Adequacy Decision system is 'cumbersome, expensive, slow, and sends a wrong message to third countries'.[376] The adequacy principle is not really a principle of data protection but it rather just serves a political need to prevent circumvention of EU law.[377] Kuner would suggest that increasing accountability and allowing individuals easier access to enforce their rights and redress would be an alternative to the Adequacy Decisions. Because of the difficulty of enforcing EU data protection rules outside the EU, the adequacy systems does not work, and instead accountability option he suggests would allow data subjects to seek remedy in their own country.[378] Data subject must be given realistic opportunities to seek redress.[379] Transparency is also a key in enforcing data protection rights in cross-border situations.[380]

[374] WP29 Opinion 01/2016, p. 27.
[375] Letter to Vice President Reding, 10.4.2014, pp. 4–5.
[376] Kuner, (2014), p. 263.
[377] Kuner, (2014), p. 267.
[378] Kuner, (2015), p. 269–271.
[379] Kuner, (2014), pp. 269–272.
[380] Kuner, (2011), p. 30.

Considering that the current Data Protection Directive and the new GDPR both require that transfers can only take place when the level of protection in the destination country is adequate, the departure from the Adequacy Decision system would require a legislative change. And I do not see how such a change could take place any time soon, despite it could be a solution in the long run.

As for increasing accountability and transparency, I see them as very good suggestions. As I have argued in this thesis, the Privacy Shield does not, despite its multiple redress options, still offer satisfactory opportunities to seek redress. The question is, how to offer realistic opportunities to redress. As this research has shown, different redress routes of the Privacy Shield lead to slightly different results, which in my view is a weakness. EU data subject ought to have the same opportunity to seek effective compensation despite the recourse route chosen by the US company. As I have stated, I do not see that ADR as such is necessarily the problem. Rather, access to ADR ought to be the same in all disputes. Likewise, access to judicial dispute resolution should not be a difficult as it is.

My own view is that the major weakness with the redress mechanisms of the Privacy Shield is its complexity. This is why, my own suggestion would be to simplify the system drastically. At the moment there seems to be too many options, instead there ought to be just instance where EU data subjects could turn to seek advice on how to seek redress. A natural solution would be that the DPAs would have this advisory role, since they already have knowledge in data protections issues. And since the legislative changes taking place, with the becoming of applicable of the GDRP, that gives national DPA more extensive powers, it would be suitable.[381]

I do think that access to courts, even European, ought not to be restricted. Still I would encourage ADR as an alternative. However, contrary to what the Privacy Shield now offers, all EU data subjects ought to have the same ADR option available, and that ought not to be dependent on the US organisation. I questioned in my arguments, the independency of the ADR body chosen by the US organisation. In my view, the Privacy Shield Panel, where the arbitrators are chosen from a pool nominated by the DoC and the Commission seems more unbiased. In that way the EU data subject would also have a choice of an arbitrator like the US company. Instead of last resort, I would prefer if the arbitration option was available immediately, or at least after consultations with the company itself. Hence, I think all EU data subject ought to have the opportunity to seek redress through arbitration. Likewise this arbitration tribunal then ought to

[381] See Arts. 51–58, General Data Protection Regulation.

have the obligation to forward the matter to the FTC or the DoC, when applicable. This would solve the problem of different results with different redress routes. Also the ADR tribunals ought to then have powers to award effective remedies that could reverse or correct the effects of non-compliance. In my view, monetary remedies ought to be available, especially when the damages are pecuniary.

Although, I must add, that in my view, even mediation could be equally considerable option as arbitration. Potentially, the ADR option that thus would be available to all disputes could be also mediation. However, the differences of arbitration and mediation are not the topic of this study, so I shall not discuss it further.

Access to judicial dispute resolution should not be restricted. Instead it ought to be an option to ADR. EU data subjects should thus have the opportunity to choose between judicial and non-judicial dispute resolution, judicial execution still being available after the judgement of an ADR tribunal. The DPAs, as advisors, could inform data subjects about the pros and cons of either of this options. Because of the limitations of EU law and access to US courts in data protection issues, access ought to be allowed in European courts, although access to US courts should still be allowed, when it is possible.

These changes could solve the main problems I have found with the Privacy Shield. EU data subjects would have the opportunity to seek effective remedies, either through ADR or courts. Also the requirement of 'a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law' of Article 47(2) would more likely to be satisfied. The requirements of equality of arms, adversarial proceedings, reasoned decision and judicial execution could also be satisfied, even in ADR proceedings. Some reasonable timeframe for the ADR proceedings ought to be defined. In my view approximately 3 months is reasonable for arbitration proceedings. One has to consider the cross-border element, with the parties located on either side of the Atlantic, there are obviously some practical difficulties. However, with the digital development, online proceedings could be an option.

I am doubtful, however, whether these suggestions could be applied to disputes with US public authorities. Development in this area could require more cooperation between the EU and the US. And that cooperation could be very difficult given the fundamental differences in data protection and also the political issues involved. Although some think that the need to provide better data protection for EU citizens may shift the dynamic of global data protection and lead

the US to create more meaningful data protection laws.[382] Despite I agree that the EU has wide reaching effects on data protection on a global scale, I doubt that the US would be willing to accept EU dominance in the field and adopt EU standards of data protection.

Instead, what could be a viable solution in the long run, is a departure from the traditional geographical approach to legislation and borderless internet. Restrictions on the flow of data across borders because of privacy and data protection concerns can undermine the potential of the Internet as a commercial platform.[383] The solution for the data protection dispute could be found in the departure from the traditional geographic thinking, non-territorial forms of jurisdiction, overlapping political authorities, and harmonization through international organisations. Effective global governance can be achieved through reconceptualising of political space and jurisdiction.[384] Arguably, EU data protection would lack teeth if it did not have effects outside the EU, cross-border data flows are inevitable in the world of internet and thus legislative spill-over cannot be avoided. The traditional Westphalian international system assumes jurisdictional conflicts as exceptions, but would it not be reasonable to assume them rather as a rule in the increasing geographical ambiguity of transnational economic transactions. Reconceptualization of jurisdictional and political community may be needed.[385] The solution could thus be a completely different approach to data protection, which would not be territorial.

According to Kuner, the European Data Protection legislation is nothing but an illusion, Europeans like to think that it provides seamless protection in data transfer situations and the hands of EU laws would reach outside the border of the EU. But Kuner thinks, this is not possible in practice, since data cannot be protected on a larger scale and intelligence surveillance cannot be completely prevented. He also considerers that the Privacy Shield is weak attempt to provide complete protection with mechanism that are 'lengthy, untransparent, formalistic, and unintelligible to the average individual.'[386]

The Schrems has also been criticized for establishing unattainable and hypocritical standards. It may also undermine the authority of EU in the field of data protection.[387] Although some think that the case could have opposite effect, strengthening the role of EU as the world leader

[382] Davies, (2015), p. 58.
[383] Meltzer, (2014), p. 97.
[384] Kobrin, (2014), p. 129–130.
[385] Kobrin, (2014), p. 112–113.
[386] Kuner, (2016), p. 4.
[387] NiLoidean, (2016), p. 6.

in data protection *albeit* it might have implications on international trade.[388] Kuner thinks that EU data protection standards cannot be set so high, that is impossible for third countries to attain them. And in a pluralistic world it is necessary to leave from the local approaches, especially in the field of data protection. Also considering that the United States is liberal democracy with strong cultural and historical ties with Europe, the protection of data across the Atlantic ought to be easy. The *Schrems* judgement does not actually lead to better data protection. Kuner thinks that the case is an example of 'human rights "petrified into a legalistic paradigm"' as stated by Martti Koskenniemi.[389] Koskenniemi's argument is basically that when human rights (such as data protection) become institutionalised values and interests are marginalised to rights-language and their transformative effect is lost and they thus are 'petrified into a legalistic paradigm.'[390] This is political aim.[391] Rights are also constantly weighed against other notions of good, there is a constant conflict and any balancing exercise is done based on political and cultural preferences.[392] Rights are 'indistinguishable from policy'.[393]

Hence, a departure from the European fundamental rights approach and an attempt to enforce EU standards and instead take a step towards breaking national borders is something that I see somewhere in the distant future. However, this would require international cooperation and it would take time. Ensuring effective redress is definitely a more immediate solution. According to Max Schrems, data protection is entering an era where it needs to be effectively enforceable.[394] Given the growing importance of data, I agree. Still, seeking redress in transatlantic situations is not easy.

The political environment in the US does not seem very open to allowing crossborder dispute resolution in data protection issues. Recent developments in the United States might prove out to be disastrous for the ability of EU citizens to challenge US organisations for data breaches. In January 2017 President Donald Trump signed an Executive Order which could conflict with the Privacy Shield and threaten the attempt of the EU to strengthen data protection of EU citizens.[395] Section 14 of the Executive Order would exclude EU citizens from the protections of

[388] Varotto, (2016), p. 10.
[389] Kuner, The Sinking of the Safe Harbor, (2015)
[390] Koskenniemi, (1999), p. 99.
[391] Koskenniemi, (1999), p. 100.
[392] Koskenniemi, (1999), p. 105–110.
[393] Koskenniemi, (1999), p. 113.
[394] Schrems, (2016), p. 149–150.
[395] Schwent and Ventrone, (2017).

the Privacy Act.[396] Even though it is not legislation, the Order does raise questions which direction is the transatlantic relationship going in terms of data protection.[397]

The Privacy Shield is planned to be jointly review for the first time in the summer of 2017. This is an opportunity to make changes to the regime.[398] This is certainly called for, with the GDPR soon becoming applicable and also the specific problems that I have highlighted with regards to the redress mechanisms of the Privacy Shield.

[396] Executive Order: Enhancing Public Safety in the Interior of the United States, 25 Jan 2017, Sec. 14.
[397] Schwent and Ventrone, (2017).
[398] From Safe Harbour to Privacy Shield, (2017), p. 34.